厦门才茂 CM520-6X 系列路由器说明书

厦门才茂通信科技有限公司

厦门市集美区软件园三期诚毅北大街63号901、904单元

电话：0592-5902655　传真：0592-5975885邮政编码：361009

网址：www.caimore.com　Email:caimore@caimore.com

版权声明：

商标声明：

注意：

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

特别声明：

产品说明书上的建议配置或者默认配置，不代表合适配置，客户须根据自己业务需要情况，调整成为适应自己业务开展的配置。

产品出厂的配置参数，仅供用户参考，用户收到设备时，不管有没有其他约定，用户必须全部检查一遍，并须根据自己项目和业务需求，自行调整配置好相关参数。由于参数配置不当或者错误导致的问题，我司不承担任何责任。

同时，用户需要加强病毒攻击防范工作，因为病毒攻击导致的通信异常，我司不承担任何责任。

版本说明:

文档版本	修改说明	发布日期	作者
V1.0	第一次正式发布	2017-10-11	cyq
V1.1	添加 5G 说明	2020-07-10	Zhengfh
V1.2	部分功能说明更新	2020-01-22	Zhengfh

目录

第一章 产品简介

1.1 产品概述

设备 WIFI 2.4GHz 和 5GHz 信道选择，同时系统加载了广域网通信 VPN 隧道、WIFI 局域网传输的安全认证等安全功能，实现无线局域网和无线广域网的无缝连接，为用户提供高速、安全、可靠的移动宽带服务。设备采用高性能的工业级 MIPS 通信处理器，以嵌入式实时操作系统为软件支撑平台，系统集成了全系列从逻辑链路层到应用层通信协议，支持 VPN（包括 GRE 、PPTP、L2TP、IPSEC、OPENVPN、N2N），IPTABLE 防火墙，静态及动态路由，PPPOE，PPP server 及 PPP client，DHCP server 及 DHCP client，WiFi client,DDNS，防火墙，SNAT/DNAT，DMZ 主机，WEB 配置，支持 APN/VPDN，支持上电自动拨号，自动维护通信链路，保证链路正常在线，支持自动定时上线和下线，定时开关机（定制）等功能。

该产品整机采用工业级设计，系统带有看门狗 WDT 保护，另外加载了系统监测保护 SWP（System Watch Protect）。产品通过电力 3000V 电击测试，产品拥有维护系统稳定的专利技术，确保设备永远在线，经过严格的设计、测试和实际应用，产品性能稳定可靠。

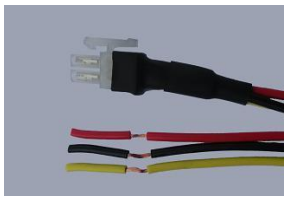
本产品已广泛应用于中小企业上网，家庭上网，金融交易，邮政交易，智能电网，智能交通，环保监测，消防监控，安防监控，水利监测，公共安全，广告发布，遥感勘测，工业控制，油田监测，煤矿监测，地震监测，气象监测，仪表监测，水表抄表，电表抄表，燃气抄表，热网监控，集中抄表等行业。

1.2 产品图片

产品接口图：

		
产品全景	正面接口	背面接口

产品配件图片：

			
车载电源接头	以太网线	串口线	可配天线

1.3 产品命名规则

公司标志	产品类别	-	硬件平台	外观结构	网络类型	-	（特殊版本）
CM	520	-	6	2	F	-	（ S ）

W：WCDMA
S：TD-SCDMA
E：EV-DO
T：LTE-TDD,LTE-FDD (EVDO,CDMA 除外)
F：LTE-TDD,LTE-FDD（全网通）
H：HSPA+
FS：5G

A：双模 5.8GWIFI
B：双模 2.4GWIFI 带 GPS
C：双模 5.8GWIFI 带 GPS
1：单模 双 WIFI
2：单模 2.4GWIFI
3：单模 5.8GWIFI
4：单模 双 WIFI 带 GPS
5：单模 2.4GWIFI 带 GPS
6：单模 5.8GWIFI 带 GPS
7：双模 双 WIFI
8：双模 双 WIFI 带 GPS
9：双模 2.4GWIFI

1.4 产品列表

主机采购信息列表：

产品名称	产品型号	2.4G WIFI	5.8G WIFI	1个WAN口 4个LAN口	2个 SIM/UIM 卡槽	1个 SIM/UIM 卡槽	1个 TF 卡槽 (卡客户购买)	GPS	SSD 固态硬盘 (客户购买)
高端车载路由器 (出厂标配)	CM520-6A		✓	✓	✓		✓		✓
	CM520-6B	✓		✓	✓		✓	✓	✓
	CM520-6C		✓	✓	✓		✓	✓	✓
	CM520-61	✓	✓	✓		✓	✓		✓
	CM520-62	✓		✓		✓	✓		✓
	CM520-63		✓	✓		✓	✓		✓
	CM520-64	✓	✓	✓		✓	✓	✓	✓
	CM520-65	✓		✓		✓	✓	✓	✓
	CM520-66		✓	✓		✓	✓	✓	✓
	CM520-67	✓	✓	✓	✓		✓		✓
	CM520-68	✓	✓	✓	✓		✓	✓	✓
	CM520-69	✓		✓	✓		✓		✓

可选配模块采购信息列表：

1、 SSD 固态硬盘，容量：64G，128G，256G，512G

1.5 产品特点

工业级设计

项目	内容
车载电源接口	车载电源接口：独有的车载电源接口设计，牢固不松脱
金属外壳设计	工业级金属外壳设计，消除火灾隐患
监控手段	带 I\O 端口，检测和报警车辆故障,GPS 车辆定位
工业级 CPU	工业级 ARM 高性能嵌入式处理；带 32 KB D-Cache，高速缓存数据，加快高速数据访问速度；带 64 KB I-Cache，高速指令缓存，加强了指令处理速度
工业级无线模块	采用工业级无线模块，抗干扰强，传输稳定
实时操作系统	采用 Linux 操作系统，带内存管理单元，实时性强，功能升级快，系统稳定，带有完善 TCP/IP 协议栈
强化电路板	PCB 采用遵循 20H 和 3W 原则，同时公司所有产品电路板都采用高品质材质来生产，确保板材的稳定可靠
工业级元器件	整机元器件采用严格筛选的工业级元器件来生产
工业级电源	宽压电源设计，电源适应范围为 DC7V - DC32V，内置电源反向保护和过压过流保护
电磁防护	以太网接口内置 1.5KV 电磁隔离防护
抗干扰设计	采用金属外壳，屏蔽电磁干扰，系统保护等级 IP31；天线带防雷设计；系统超低温和超高温设计；特别适合在环境恶劣的工业环境下使用

稳定可靠

项目	内容
车载电源接口	车载电源接口：独有的车载电源接口设计，牢固不松脱
在线维持专利技术	智能防掉线，在线检测，在线维持，掉线自动重拨，异常自动复位，确保设备永远在线
三层系统保护	在原来两级（软件保护+CPU 内置看门狗 WDT 保护）系统保护的基础上，增加一级系统虚拟值守 VWM（Virtual Man Watch）检测保护功能，确保系统稳定可靠
UIM/SIM 卡 ESD 保护	1.8V/3V/5V 标准的推杆式用户卡接口，内置 15KV ESD 保护
串口 ESD 保护	串口 RS232 内置 15KV ESD 保护
金属外壳	采用金属外壳，防辐射，抗干扰；外壳和系统安全隔离，防雷设计；符合电力安规要求；防护等级为 IP31；特别适合于环境恶劣的工业控制领域
无线模块	所有无线模块都有通过 CGD 认证或者 FCC 认证或者 CE 认证
高速处理 CPU	采用高速 ARM 的工业级 CPU，可以更加高速地处理各种协议数据转换；解决了业内“假在线”、“假死机”、“当机”等疑难问题
超大内存	DDR3/1066 容量 4Gbits,有超大的内存来缓存客户发送数据，同时接收超大数据包，数据不丢失
内存管理 MMU	新款 CPU 带内存管理 MMU，可以防止系统内存异常问题导致的系统不稳定现象
完善的协议栈	系统采用了完善的 TCP/IP 协议栈，使网络通信性能优异，掉线概率极大降低
EMC 性能优异	通过电力 3000V 电击测试，特别适合在工业领域环境恶劣下使用；通过 CE 认证，ROSH 认证，3C 认证，电信设备入网认证，铁道部 CRCC 认证

1.6 软件功能

内容
产品出厂配置默认参数，客户只需修改个别参数甚至不需要做任何参数修改，就可以实现快速使用设备
图形化配置工具：完善的图形化配置工具，提供快速配置功能，实现客户快速配置；提供批量配置功能，实现批量设备的配置
产品说明书提供快速配置说明，可以快速使用设备
检查软件：提供 SYSLOG 日志输出功能，可以用于参考设备工作日志，协助分析异常时原因；通过串口调试软件，提供不同的调试等级输出，方便客户查看各种信息，快速定位问题

项目	内容
上网功能	单 3/4G/5G 模块拨号、双 4G/5G 模块拨号，全网通模块，支持 LTE-TDD、LTE-FDD、TD-SCDMA、WCDMA、EVDO、GPRS、CMDA2000 制式网络拨号，支持 APN/VPDN 网络拨号，智能防掉线，支持在线检测，在线维持，掉线自动重拨，确保设备稳定在线
	有线接入，支持静态 ip 上网、DHCP 客户端、PPPOE 拨号
	WIFI 客户端模式
	有线为主，无线为辅工作模式
	交换机工作模式
	支持 mwan3 带宽叠加功能
局域网功能	4 个 LAN 局域网 1000M 网口
	双 WiFi 模块，2.4G/5G 可设置切换，支持 802.11a/b/g/n/ac 标准协议，支持接入点 AP、客户端 client、点对点 Ad-Hoc、接入点 AP(WDS)、客户端 client(WDS)、静态 WDS 工作模式。
	全网通模块，支持 LTE-TDD、LTE-FDD、TD-SCDMA、WCDMA、EVDO、GPRS、CMDA2000 制式网络拨号，支持 APN/VPDN 网络拨号
	支持 dnsmasq 功能，实现 DNS 服务器、DHCP 服务器
高级功能	支持端口映射 NAT 功能和 DMZ 主机，如 SNAT，DNAT
	支持静态路由配置
	支持 TCP/IP，UDP，ICMP，SMTP，HTTP，POP3，OICQ，TELNET，FTP 等协议
	支持 ntp 网络时钟
	支持 IPTABLES 防火墙，包过滤功能
	支持 QOS 网络质量管理
	支持动态 DDNS：支持花生壳、88IP 和 dyndns 域名服务商
	支持花生壳内网版
	支持网络限速、流量监控，QOS 网络质量管理，用户应用过滤功能
VPN 功能	支持 PPTP 客户端功能,PPTPD 服务端功能
	支持 L2TP 客户端功能,L2TPD 服务端功能
	支持 IPSEC 功能
	支持 OPENVPN 功能
	支持 N2N 功能

设备管理	本地 web 管理，从局域网默认配置 192.168.9.1:9999 进入配置页面
	本地固件升级，可根据需要选择是否保存配置参数
	支持 SSH 管理，方便易用的控制台 shell 交互环境
	支持串口本地软件升级
	方便易用的 COM 及 SYSLOG 系统诊断，调试功能
	系统状态查看，查看当前设备工作状态、各个工作网口的数据上下行数据包数量、VPN 工作状态等
	支持 3 路控制输出；可以控制车辆熄火等（非标配需定制）
公共 WiFi 运营功能	支持 WIFI 嗅探功能，嗅探终端的 MAC 上报到平台分析统计
	支持用户 URL 抓取，上报到平台分析统计
	支持本地广告推送功能
	支持如影随形广告功能
	支持精准广告推送功能
	支持本地 web 服务器，内嵌 nginx+php+mysql 服务
	支持站点更新多媒体功能，车辆到达站点利用站点的 WiFi 进行更新多媒体资源，节省 4G/5G 流量，也加快更新速度，支持断点续传功能
	支持 WiFidog portal 功能、支持一键认证、微信认证、短信认证和本地认证等方式
远程平台管理	远程设备状态查看
	远程设备参数批量配置
	远程设备固件批量升级
	远程设备多媒体批量更新
	远程设备分组管理、流量控制
	远程设备数据上报分析统计报表
存储方式	支持一张 TF 卡，最大可达 256G（预留接口，暂不支持）
	支持一个 SSD 固态硬盘，最大可到 2T（依市面而定）
定位功能	支持 GPS/北斗定位（非标配，采购时需额外告知）

1.7 硬件参数

硬件系统：

项目	内容
CPU	工业级高性能 ARM 嵌入式处理器 CPU，主频 1.4Ghz(双核)，副频 733Mhz(双核)
MMU	CPU 带 MMU 内存管理单元，可以防止内存溢出导致系统的异常
FLASH	NOR FLASH 256Mbit，有足够大的内存来存放程序和数据
DDR3	内存支持 32bit DDR3/4G-16Gbits，有足够大的缓存来提高系统运算速度
SSD 固态硬盘	支持最高 2T 大容量固态硬盘，可存储资源更加丰富

操作系统：

项目	内容
操作系统	采用 Linux 操作系统，带内存管理单元，实时性强，功能升级快，系统稳定

接口类型：

项目	内容
WAN 口	1个10/100/1000M自适应WAN口，支持自动翻转（Auto MDI/MDIX），支持PPPOE
以太网口	4个10/100/1000M自适应LAN口，支持自动翻转（Auto MDI/MDIX），内置1.5KV电磁隔离保护
串口	1 个 RS232 或 RS485 接口 数据位：7、8 位 停止位：1、2 位 校验位：无校验、奇校验、偶校验 波特率：300bps - 115200bps 流控：无流控
指示灯	电源指示灯 SYS 系统指示灯 链路 1 在线状态指示灯 链路 2 在线状态指示灯 链路 1 无线信号指示灯 链路 2 无线信号指示灯
天线接口	标准 SMA 阴头天线接口，特性阻抗 50 欧 可以选配 1M/3M/5M/10M 的天线延长线，满足不同使用场合需要
UIM 卡接口	1.8V/3V/5V 标准的推杆式用户卡接口，内置 15KV ESD 保护
电源接口	航空头接口或者车载接口
RESET 按键	恢复出厂设置按键
TF 卡接口	支持 32-256G

供电情况：

项目	内容
供电电压	宽电压设计，DC 7V - DC 32V 电源都可以直接给设备供电； 同时内置电源反向保护和过压过流保护
标配电源	DC:9V/1.5A
通信电流	通信时平均电流：390mA@+9VDC 登网瞬间峰值电流：1.0A@+9VDC
待机电流	待机平均电流：< 56mA@+9VDC
动车供电系统	110V 支持/汽车取电/220V 适配器取电

物理特性：

项目	内容
外壳	采用金属外壳，防辐射，抗干扰 外壳和系统安全隔离，防雷设计 符合电力安规要求 防护等级为 IP30 特别适合于环境恶劣的工业控制领域
产品外形尺寸	228*144*35mm（不包括天线及固定件）
产品包装尺寸	340*327*80mm
重量	1.02kg
天线	8 个 RP-SMA
供电	峰值功耗≤12W　平均功耗 9W 电源适配器 12V DC，+/-10%
温度	工作温度：-25℃ ～ 70℃ 扩展工作温度：-30℃ ～ 75℃ 存储温度：-40℃ ～ 80℃
湿度	工作湿度：5%～95% （非凝结） 存储湿度：0%～100% （非凝结）
防护等级	IP31
认证	CCCI 认证

无线参数：

4G 5G 无线技术参数	
无线模块	采用工业级无线模块
标准及频段（支持国外频段）	5G NR:n1/n2/n3/n5/n7/n8/n20/n28/n41/n66/n71/n77/n78/n79 LTE TDD: Band 38/39/40/41 LTE FDD: Band 1/2/3/4/5/7/13/17/25 TD-SCDMA: Band 34/39 GSM: Band 2/3/8 UMTS: Band 1/5
编码方案	LTE/UMTS/HSPA+/DC_HSPA+/HSDPA/HSUPA/WCDMA/EDGE/GSM
理论带宽(DL:下载速率、UL 上传速率)	5G NR: DL 3.4Gbps/UL 350Mbps LTE TDD: DL 61Mbps/UL 18Mbps LTE FDD: DL 100Mbps/UL 50Mbps DC_HSPA+: DL 42Mbps/UL 5.76Mbps HSPA+: DL 28Mb/s(Category 18) HSDPA: DL 14.4Mb/s(Category 8) HSUPA+: DL 42Mbps/UL 5.76Mbps WCDMA CS: DL 64kbps/UL 64kbps WCDMA PS: DL 384kbps/UL 384kbps EDGE: DL 237Kbps/UL 118Kbps GSM: DL 171Kbps/UL 171Kbps
发射功率	WCDMA/HSDPA: 24dBm LET: 23 dBm
接收灵敏度	<-109dBm
功能支持	支持数据、语音、短信和传真

联通 3G 无线技术参数	
无线模块	采用工业级无线模块
通信带宽	HAPA+: DL 21Mbps/UL 5.76Mpbs HSDPA/HSUPA: DL 7.2Mbps/UL 5.76Mbps WCDMA: DL 384Kbps/UL 384Kbps EDGE: DL 237Kbps/UL 118Kbps GPRS: DL 85.6kbps/UL 85.6kbps CSD: UL 14.4kbps
发射功率	<24dBm
接收灵敏度	<-109dBm
功能支持	支持数据、语音、短信和传真

移动 3G 无线技术参数	
无线模块	采用工业级无线模块

标准及频段	TD-SCDMA：2010~2025MHz GSM/GPRS/EDGE：850/900/1800/1900MHz 支持 3GPPclass B
编码方案	TD-SCDMA/HSDPA/HSUPA/EDGE/GPRS 模式
通信带宽	DL 2.8Mbps/UL 384Kbps
发射功率	<24dBm
接收灵敏度	<-108dBm
功能支持	支持数据、语音、短信和传真

电信 3G 无线技术参数

无线模块	采用工业级无线模块
标准及频段	支持 IS-95 A/B, CDMA2000 1XrTT,and 1X EV-DO(Revision 0 and A) 800MHz 单频，可选 800/1900MHz 双频，450MHz 单频
编码方案	IS-95 A/B, CDMA2000 1XrTT,and 1X EV-DO 模式
通信带宽	上行速率 (up to 3.1Mbps) 上行速率 (up to 1.8Mbps)
发射功率	<23dBm
接收灵敏度	<-107dBm
功能支持	支持数据、语音、短信和传真

WIFI 无线参数：

项目	内容
WIFI 模块	802.11b/g/n 双频 3×3 MIMO（450Mbps） 802.11 ac 双频 3×3 MIMO（1.3Gbps）
WIFI 工作频段	802.11b/g/n 2.412~2.472GHz，13 个信道（3 个非重叠信道） 802.11a/n 5.180～5.825 GHz
WIFI 输出功率	整机 23dBm
MTBF	≥100,000 小时
用户数量	单频支持同时 150 个用户接入，双频支持同时 253 个用户接入。
安全参数	支持 64/128 位 WEP 加密 支持 WPA-PSK/WPA2-PSK 认证类型 支持 TKIP、CCMP/AES 加密算法
传输距离	室外无阻拦/空旷，覆盖范围可达 150 米

GPS 参数：

项目	内容
模块	采用工业级 GPS/北斗模块
接收机类型	接收全球定位系统， 50 个频道， L1 的频率，1.023 兆赫芯片速度，C / A 码 1.023 兆赫芯片速度； 支持 SBAS:WAAS,EGNOS,MSAS,兼容 GALILEO
定位精确度	Position：2.5m CPE SBAS:2.0m CPE
速度精度	速度精度 < 0.01 米/秒（高速）<0.01° (heading)， （ 50 % @ 30 米/秒）
时间精度	1 微妙同步 GPS 时间
捕捉时间	冷启动：27S；辅助启动:<3 秒；热启动：<1 秒
数据格式	NMEA-1083,SiRD 二进制
输入信息	NMEA,SiRF 二进制 高度/位置/日期/时间
输出信息	NMEA-0183,SiRF 二进制，GGA GSA GSV RMC VTG GLL
秒脉冲输出	1pps 精度±1us
导航数据更新速率	5Hz
灵敏度	跟踪：-162dBm；冷启动：-147dBm；热启动：-156dBm

1.8 指示灯说明

指示灯说明：

指示灯	状态	说明
POWER 电源指示灯	电源指示灯亮	设备电源正常
	电源指示灯灭	设备未上电
SYS 系统指示灯	系统指示灯闪烁	有程序运行
	系统指示灯灭	没有程序运行
Online1（SIM 卡 1）	Online1 指示灯亮	设备已登录网络
	Online1 指示灯灭	设备未登录网络
Online2（SIM 卡 2）	Online2 指示灯亮	设备已登陆网络
	Online2 指示灯灭	设备未登录网络
信号指示灯 1	信号指示灯 1-1 灭， 1-2 灭	SIM 卡 1 的信号<12
	信号指示灯 1-1 亮， 1-2 灭	SIM 卡 1 的信号≥12 且<25
	信号指示灯 1-1 亮， 1-2 亮	SIM 卡 1 的信号≥25
信号指示灯 2	信号指示灯 2-1 灭， 2-2 灭	SIM 卡 2 的信号<12
	信号指示灯 2-1 灭， 2-2 灭	SIM 卡 2 的信号≥12 且<25
	信号指示灯 2-1 灭， 2-2 灭	SIM 卡 2 的信号≥25

第二章 安装说明

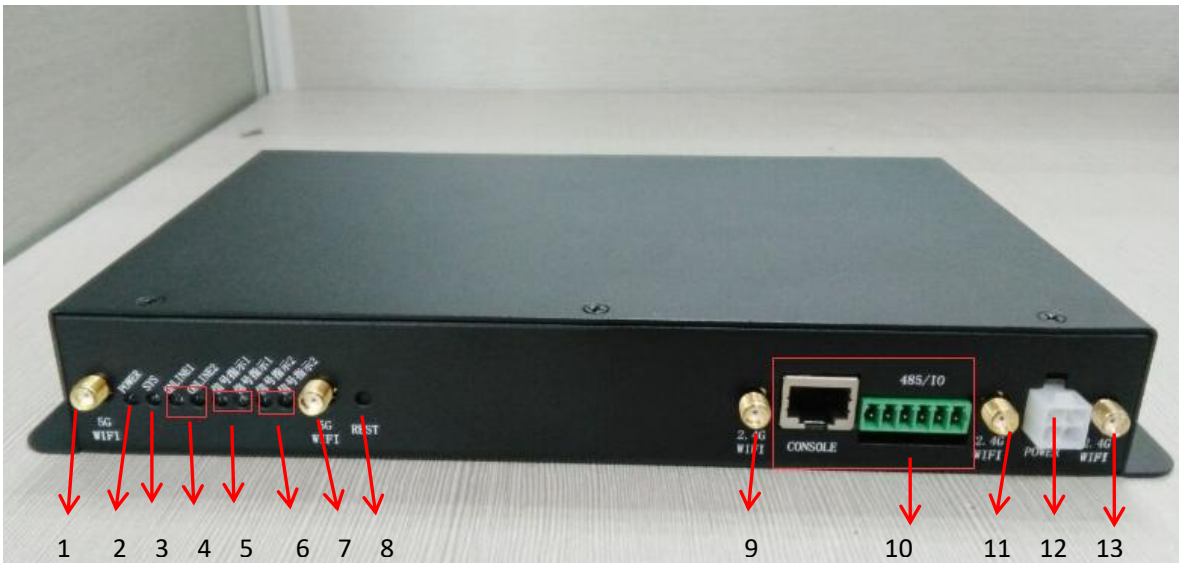
2.1 装箱清单

感谢您选择才茂通信产品，当您打开产品的包装盒后，请核对里面的物品是否与装箱清单所列一致。出厂时在包装盒内的标准配置如下：

网关主机	1 台
RJ45-DB9 线	1 根
DC 9V 电源适配器	1 个
网络直连线	1 根
3G/4G/5G天线	2 条(5G 4 根天线)
5.8G WIFI天线	3 条
2.4G WIFI天线	3 条
产品说明书光盘	1 个

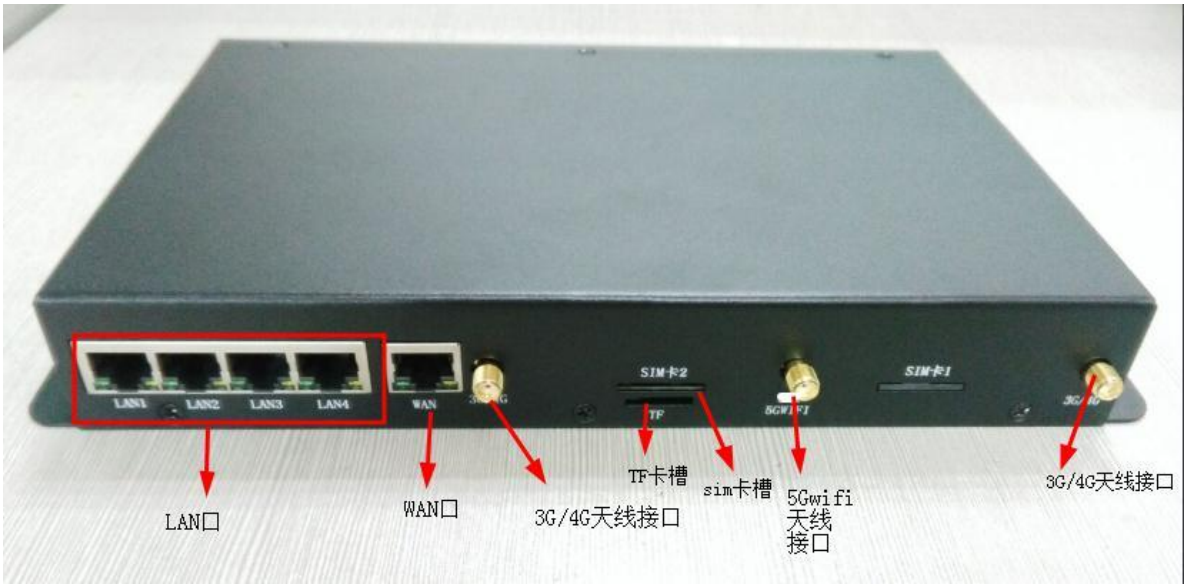
2.2 产品说明

前置面板：



1：5GWiFi 天线接口　2：电源灯　3：进程灯　4：sim 卡 1，sim 卡 2 上线灯　5：sim 卡 1 信号指示灯　6：sim 卡 2 信号指示灯　7：5GWiFi 天线接口　8：复位键　9、11、13：2.4GWiFi 天线接口　10：串口　12：电源插口

后置面板：



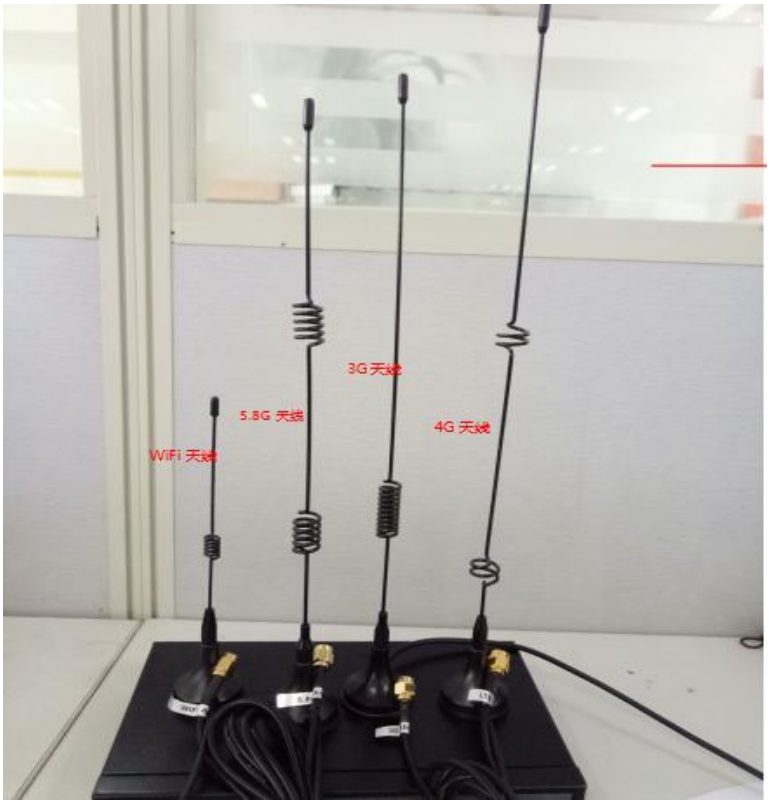
2.3 SIM 卡安装

手机 SIM 卡存储用户标识、电话号码簿、网络设置、附加服务等信息。 网关支持 1.8V/3V/5V SIM 卡， SIM 卡接口插座使用自弹式的 SIM 卡座，用户可以在不打开机壳的情况下方便地安装 SIM 卡。
安装方法：

在未上电的情况下，将 SIM 卡有金属触点的一面朝下，有缺角方向往内，水平推进 SIM 卡座上按一下让 SIM 卡固定在卡座上，如图：

警告：禁止带电拔插 SIM 卡

2.4 天线安装



第三章 快速配置

一方面为了方便客户在收到设备时，能快速检测无线网关设备是否是完好的，是否能正常工作的；另一方面，针对大部分客户只需要修改快速配置中的配置参数，其他参数使用我司出厂默认参数，便可以满足客户的使用功能要求，为了达到这两个要求，我们专门制作快速配置使用说明。下面以 Windows 7 为例，讲解工业级无线网关的快速配置过程。

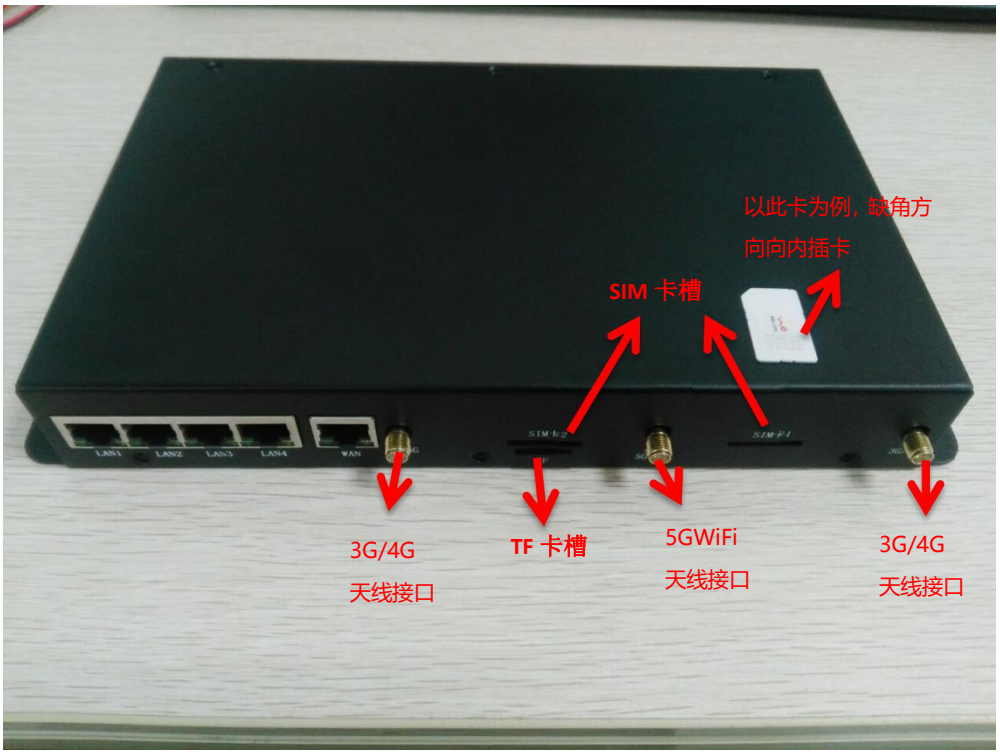
快速配置一般只需要配置 WAN 参数和 LAN 参数，其他参数直接使用工厂出厂默认参数，不需要修

改；如果需要修改其他参数，则参见《第四章 详细参数配置》。

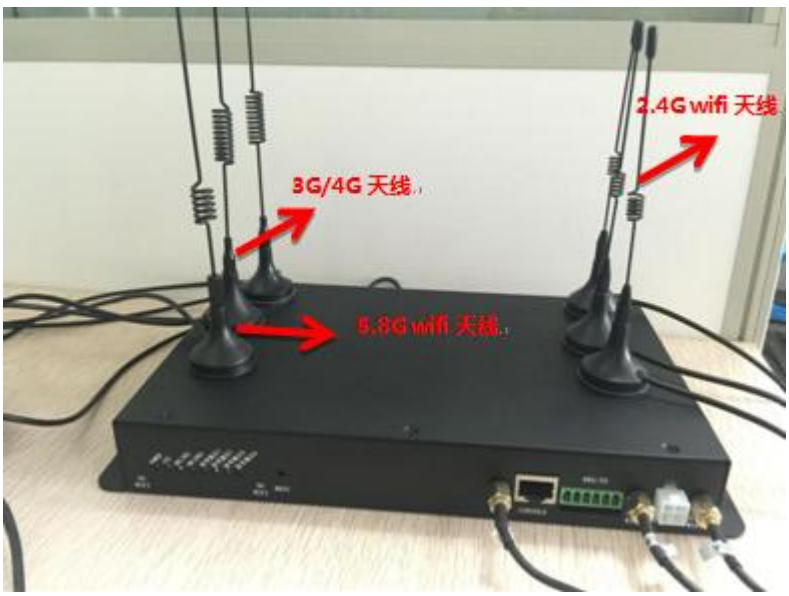
配置步骤：

3.1 拨号上网（PPPOE disable）模式

3.1.1 先将 SIM 卡插入网关 SIM 卡座



3.1.2 连接好天线

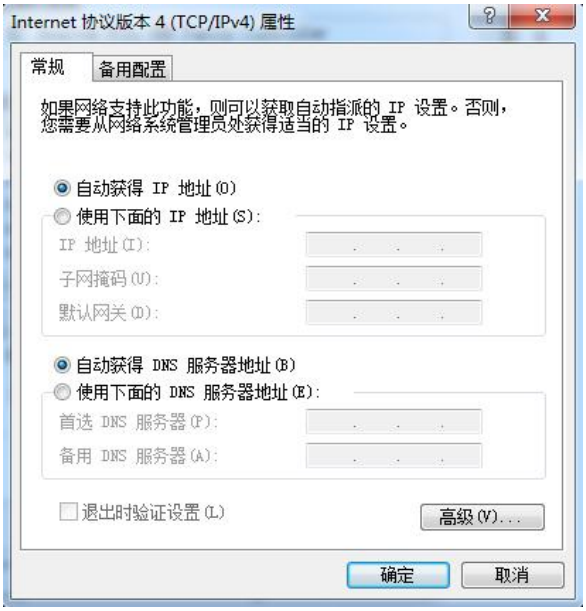


3.1.3 无线网关与 PC 硬件连接

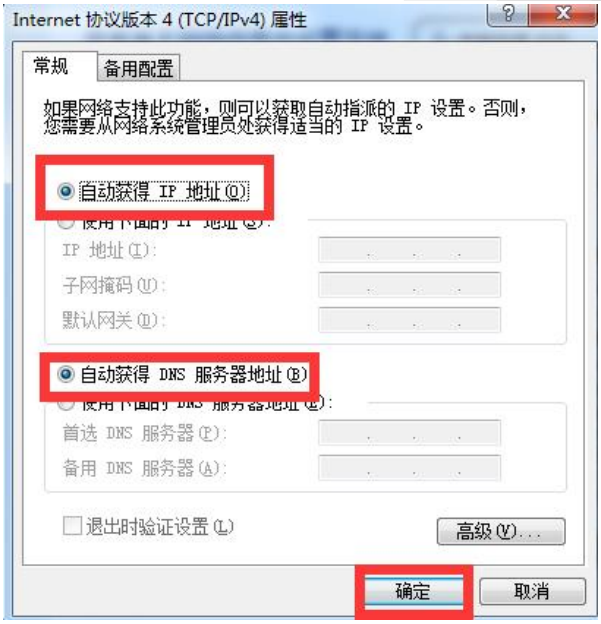
PC 通过以太网线与网关设备 LAN 口直连，如下图所示：

3.1.4 PC 端网络设置（配置 IP 地址，网关，DNS）

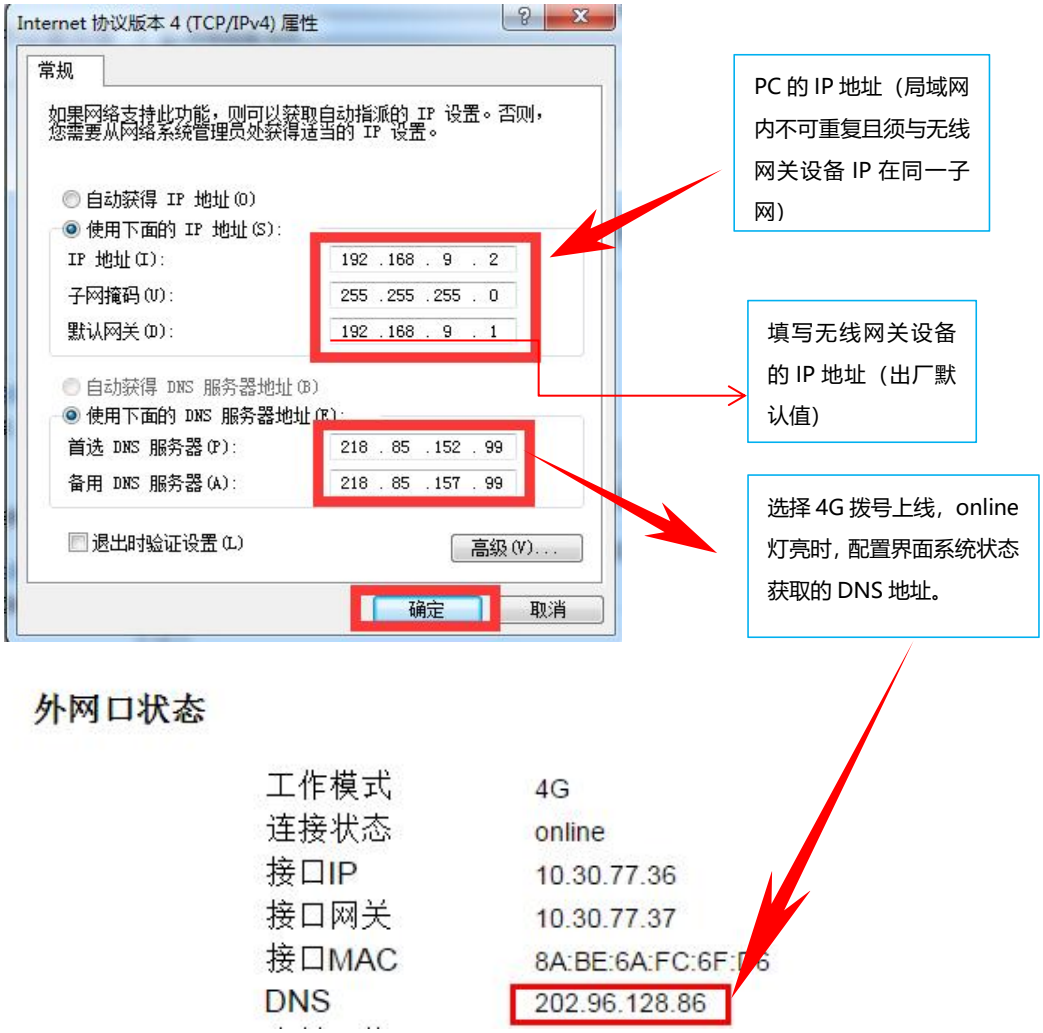
点击Windows的“开始” → “控制面板”→“网络与Internet”→“网络和共享中心”→“本地连接”→“属性”→选择双击“Internet 协议版本4 (TCP/IP)”如图：



方式 1：采用自动获取 IP、DNS


Internet 协议版本 4 (TCP/IPv4) 属性
常规
备用配置
如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，
您需要从网络系统管理员处获得适当的 IP 设置。
自动获得 IP 地址(O)
IP 地址(I):
子网掩码(U):
默认网关(D):
自动获得 DNS 服务器地址(B)
首选 DNS 服务器(P):
备用 DNS 服务器(A):
退出时验证设置(L)
高级(V)...
确定
取消

方式 2：采用静态 IP，使用固定 DNS



如果使用的 SIM 卡一直不变，就可以不用再改 DNS，如果更换不同类型 SIM 卡重复以上步骤查看 DNS。

本示例参数设置为：

无线网关 LAN1 口 IP 地址：192.168.9.1（出厂默认值）

PC 端参数设置为：

IP 地址：192.168.9.X（X 为 2-254 的任意值，本例的 X 值为 2）

子网掩码：255.255.255.0（根据 IP 地址不同，设置不同子网掩码）

默认网关：192.168.9.1（即无线路由器 LAN1 口 IP 地址：192.168.9.1）

3.1.5 配置 WAN 信息

打开“IE”,在地址栏输入192.168.9.1或者192.168.9.1:9999（网关设备出厂的LAN口默认IP地址）。如图：

输入用户名及密码（默认用户名：admin,密码：admin）。如图：

选择WAN配置,根据运营商提供的信息配置并提交，（如图是EVDO/CDMA登网的信息）。

网络	中心号码（APN）	接入点	用户名	密码
GPRS	*99***1#	cmnet(移动) uninet(联通)	为空	为空
EDGE	*99***1#	cmnet	为空	为空
TD-SCDMA	*98*1#	cmnet	为空	为空
CDMA	#777	为空	card	card
EV-DO	#777	为空	card	card
WCDMA	*99#	3gnet	为空	为空

注意：正常情况下使用我们公司出厂的默认参数就可以,不用修改，只有使用APN/VPDN专网才需要修改这项配置。3G以上面为例，4G默认放空。

3.1.6 上网测试设备

- 设备重新上电
- Sys 灯闪烁。
- 等待“Online”灯亮起来
- “Online”灯亮起来，打开网页，可以浏览网站内容，表示可以成功上网，进行无线数据传输。

3.2 WAN 口上网（Wan APclient)模式

3.2.1 接好天线

3.2.2 网关设备 WAN 口通过以太网线与广域网相连

如图：

3.2.3 PC 端网络配置（IP、网关、DNS）

3.2.4 配置 WAN 信息

打开 IE 浏览器→输入 192.168.9.1 或者 192.168.9.1：9999→输入用户名，密码→登录设备→打开 WAN 配置，如图：

3.2.5 LAN 配置

进入配置界面→打开 LAN 配置,如图：

3.2.6 上网测试设备

- 设备重新上电
- Sys 灯闪烁
- 等待“Online”灯亮起来
- “Online”灯亮起来，打开网页，可以浏览网站内容，表示可以成功上网，进行无线数据传输。

3.3 技术支持

若产品使用过程中出现问题或者遇到不解问题可以登录我司官网：http://www.caimore.com
联系我司在线技术支持人员，或者联系技术支持电话：
0592-5908951/3799892。

第四章 详细参数设置

4.1 网络配置

4.1.1 WAN 配置

网关实现上网的配置，即连接网络的基本参数。

4.1.1.1 静态 IP 地址

图 4-1-1

- **IPv4地址：**此IP应与能提供上网的广域网（外网）在同一个子网。
- **IPv4子网掩码：**设置网关设备的子网掩码。
- **MAC地址：**无需配置，系统会自动分配一个MAC地址，若需使用固定的MAC地址，则需手动配置。
- **网关地址：**默认网关为广域网所处子网对应的网关地址。
- **DNS服务器：**可以填广泛应用大型搜索引擎的DNS，如：谷歌的DNS(8.8.8.8)，百度的DNS，或者提供网络的运营商的DNS。

4.1.1.2 DHCP 客户端

图 4-1-2

- **DHCP 客户端：**网关设备使用自动获取 IP 方式上网。

4.1.1.3 PPPOE

图 4-1-3

- **用户名：**连接到公网的用户名，由运营商提供。
- **密码：**连接到公网的密码，由运营商提供。

4.1.1.4 4G/5G 拨号

图 4-1-4

- **拨号中心号码、接入点、用户名、密码：**出厂时已经根据网络进行默认设置（参见附录5）通常情况下，不需要修改这些信息。如果使用VPND，则请根据运营商提供拨号中心号码、接入点、用户名和密码的信息填入对应的输入框中。4G/5G默认放空。
- **搜网模式：**默认为自动，一般无需更改。若长时间拨不上号，可更改为对应网络的搜网模式。

4.1.1.5 主辅模式

图 4-1-5

- **主模式：**可选择静态IP地址、DHCP客户端、PPPoE三种模式。
- **静态IP、PPPoE拨号、SIM卡拨号1：**设置同上所述。

该模式下优先选用主模式上网,若主模式无法连接，则选用SIM卡拨号上网。

4.1.1.6 交换机模式

图 4-1-6

- **交换机模式：**网关设备作为交换机使用。

4.1.1.7 双模路模式

图 4-1-7

- SIM卡拨号1、SIM拨号2：设置同上所述。

该模式下双模块同时上网，进行带宽叠加。

注：

若安装双模块的设备选用 4G/5G 拨号上网，则优先识别 SIM 卡 2 接入的模块，故只有一张 SIM 卡时，需插入 SIM 卡 2 的卡槽进行上网。

4.1.1.8 WiFi 客户端模式

图 4-1-8

- SSID：所连WIFI的网络标识。
- 密码：所连WIFI的密码。

注：

所连 wifi 的 IP 网段不能与该设备的 LAN 网段相同。

4.1.2 LAN 配置

图 4-1-9

- **IP地址**：指网关WIFI、LAN1-4接口IP地址，默认IP地址为192.168.9.1。
- **子网掩码**：设置本地IP地址对应的子网掩码。
- **MAC地址**：本网关的LAN1-4的MAC地址。无需设置，系统会自动分配。
- **首选DNS/备用DNS**：指域名解析服务器的地址，默认情况下已填写，如果客户有稳定的DNS服务器，可以填入客户知道的稳定的DNS服务器地址。

注：

1、必须确保相连设备的IP地址与网关在同一个子网内。

2、当多台我司的无线网关在同一个局域网时，MAC地址在“载入出厂设置”后将会恢复成出厂值，这样容易导致MAC地址和其他设备的相冲突。所以请修改MAC地址。

3、如果填写DNS服务器地址，请在拨号完成后，检测网关所使用的DNS,能否正确解析域名。

4.1.3 WiFi 配置

4.1.3.1 2.4GWiFi 配置

图 4-1-10

- **信道**：选择设备将使用的工作频率。除非发现与附近其它接入点之间存在干扰问题，否则不必更改无线频道。优先选择频道 1、6、11。
- **无线功率**：从某方面理解其实就是无线路由器无线网络覆盖的范围。功率越大，网络覆盖范围也就越大。
- **模式**：选择设备要工作的模式。
  802.11 b ： 只支持 b 的无线客户端连接。
  802.11 g ： 只支持 g 的无线客户端连接。
  802.11 a ： 只支持 a 的无线客户端连接。
  802.11 g+n mixed ： 支持 g 或 n 的无线客户端连接。
  802.11 a+n mixed ： 支持 a 或 n 的无线客户端连接。
  802.11 ac mixed ： 支持 ac 的无线客户端连接。
- **频宽**：信号所拥有的频率范围叫做信号的频带宽度，保证某种发射信息的速率和质量所需占用的频带宽度容许值。
- **国家代码**：一组用来代表国家和境外领土的地理代码，国家代码是由字母或数字组成的短字串，方便用于数据处理和通讯。
- **距离优化**:默认。
- **分片阈值**:默认。
- **RTS/CTS 阈值**:默认。
- **模式**：可选择接入点 AP、客户端 Client、Wireless Repeate。
- **ESSID**：标识无线网络的网络名称。最大支持 32 个字符，默认为 CaiMore_WiFi_2G,建议修改，以免在网络搜索范围内与我司提供的同类产品冲突。
- **BSSID**：BSSID 实际上就是 AP 的 MAC 地址，用来标识 AP 管理的 BSS。
- **隐藏 SSID**：可选择是否隐藏 SSID，若隐藏，则无法搜索到该设备 WiFi，但已连接到该设备 WiFi 的终端不会断开连接。
- **加密方式**：
  None：无数据加密，即开放式网络，设备连接至 AP 无需密码验证。
  WEP 开放认证：采用 WEP 标准加密，使用开放式系统认证。

WEP 共享密钥：采用 WEP 标准加密，使用共享密钥认证。

WPA-PSK：采用 WPA-PSK 标准加密，使用预共享密钥保护访问。

WPA2-PSK：采用 WPA2-PSK 标准加密，使用预共享密钥保护访问。加密类型　　AES。

WPA-PSK/WPA2-PSK Mixed Mode：采用 WPA-PSK 或 WPA2-PSK 标准加密，使用预共享密钥保护访问。

下列将对安全选择进行说明：

WEP 开放认证：

图 4-1-12

- **密码#1：**密钥，长度可分 5、13、16 个字符。

WEP 共享密钥：

图 4-1-13

- **密码#1：**密钥，长度可分 5、13、16 个字符。

WPA-PSK 加密：

图 4-1-14

- **加密方式：**支持自动、强制使用 CCMP(AES)加密、强制使用 TKIP 加密、TKIP 和 CCMP(AES)混合加密。
- **密码：**密钥，长度介于 8 ~ 63 个字符之间。

WPA2-PSK 加密：

图 4-1-15

- **加密方式：**支持自动、强制使用 CCMP(AES)加密、强制使用 TKIP 加密、TKIP 和 CCMP(AES)混合加密。
- **密码：**密钥，长度介于 8 ~ 63 个字符之间。

WPA-PSK/WPA2-PSK Mixed Mode:

图 4-1-16

- **加密方式：**支持自动、强制使用 CCMP(AES)加密、强制使用 TKIP 加密、TKIP 和 CCMP(AES)混合加密。
- **密码：**密钥，长度介于 8 ~ 63 个字符之间。

4.1.3.2 5GWiFi 配置

图 4-1-17

- **信道：** 选择本设备将使用的工作频率。除非发现与附近其它接入点之间存在干扰问题，否则不必更改无线频道。优先选择频道 1、6、11。
- **功率：**从某方面理解其实就是无线路由器无线网络覆盖的范围。功率越大，网络覆盖范围也就越大。
- **模式：**选择本设备要工作的模式。
  802.11 b ： 只支持 b 的无线客户端连接。
  802.11 g ： 只支持 g 的无线客户端连接。
  802.11 a ： 只支持 a 的无线客户端连接。
  802.11 g+n mixed ： 支持 g 或 n 的无线客户端连接。
  802.11 a+n mixed ： 支持 a 或 n 的无线客户端连接。
  802.11 ac mixed ： 支持 ac 的无线客户端连接。
- **频宽：**信号所拥有的频率范围叫做信号的频带宽度，保证某种发射信息的速率和质量所需占用的频带宽度容许值。
- **国家代码：**一组用来代表国家和境外领土的地理代码，国家代码是由字母或数字组成的短字串，方便用于数据处理和通讯。
- **距离优化：**
- **分片阈值：**
- **RTS/CTS 阈值：**
- **模式：**可选择接入点 AP、客户端 Client、Wireless Repeater。
- **ESSID:**标识无线网络的网络名称。最大支持 32 个字符，默认为 CaiMore_WiFi_5G,建议修改，以免在网络搜索范围内与我司提供的同类产品冲突。
- **BSSID:** BSSID 实际上就是 AP 的 MAC 地址，用来标识 AP 管理的 BSS。
- **隐藏 SSID：**可选择是否隐藏 SSID，若隐藏，则无法搜索到该设备 WiFi，但已连接到该设备 WiFi 的终端不会断开连接。
- **加密方式：**
  None：无数据加密，即开放式网络，设备连接至 AP 无需密码验证。
  WEP 开放认证：采用 WEP 标准加密，使用开放式系统认证。
  WEP 共享密钥：采用 WEP 标准加密，使用共享密钥认证。
  WPA-PSK：采用 WPA-PSK 标准加密，使用预共享密钥保护访问。
  WPA2-PSK：采用 WPA2-PSK 标准加密，使用预共享密钥保护访问。加密类型 AES。
  WPA-PSK/WPA2-PSK Mixed Mode: 采用 WPA-PSK 或 WPA2-PSK 标准加密，使用预共享密钥保护访问。

下列将对安全选择进行说明：

WEP 开放认证：

图 4-1-18

- **密码#1：**密钥，长度可分 5、13、16 个字符。

WEP 共享密钥：

图 4-1-19

- **密码#1**：密钥，长度可分 5、13、16 个字符。

WPA-PSK 加密：

图 4-1-20

- **加密方式**：支持自动、强制使用 CCMP(AES)加密、强制使用 TKIP 加密、TKIP 和 CCMP(AES)混合加密。
- **密码**： 密钥，长度介于 8 ~ 63 个字符之间。

WPA2-PSK 加密：

图 4-1-21

- **加密方式**：支持自动、强制使用 CCMP(AES)加密、强制使用 TKIP 加密、TKIP 和 CCMP(AES)混合加密。
- **密码： 密钥，长度介于 8 ~ 63 个字符之间。**

WPA-PSK/WPA2-PSK Mixed Mode:

图 4-1-22

- **加密方式**：支持自动、强制使用 CCMP(AES)加密、强制使用 TKIP 加密、TKIP 和 CCMP(AES)混合加密。
- **密码**：密钥，长度介于 8 ~ 63 个字符之间。

4.1.4 DHCP 配置

DHCP指动态主机控制协议(Dynamic Host Control Protocol)。能够自动分配IP地址给局域网中的计算机。对用户来说，为局域网中的所有计算机配置TCP/IP协议参数并不是一件容易的事，它包括IP地址、子网掩码、网关、以及DNS服务器的设置等。若使用DHCP服务则可以解决这些问题。系统默认为启用，如果不需要DHCPD服务，请关闭此选项。

图 4-1-24

- **起始分配基址：**该项为DHCP服务器自动分配IP地址时的起始地址。
- **客户数：** DHCP服务器自动分配IP地址的个数。

4.1.5 VLAN 配置

可以将局域网划分成多个VLAN。

图 4-1-23

每个端口在分组中有三个选项：关、不关联、关联。

- **关**：这一分组中不适用这个接口。
- **不关联**： 这个接口将被直接桥接到这个分组。
- **关联**：这个接口需要通过VLAN ID来访问这一分组。

注：非专业人士请勿轻易配置VLAN。

4.2 高级配置

4.2.1 静态路由

完成系统静态路由设置和显示系统路由信息。系统默认路由即把所有的数据送往公网，如需访问指定网络请手动添加路由。

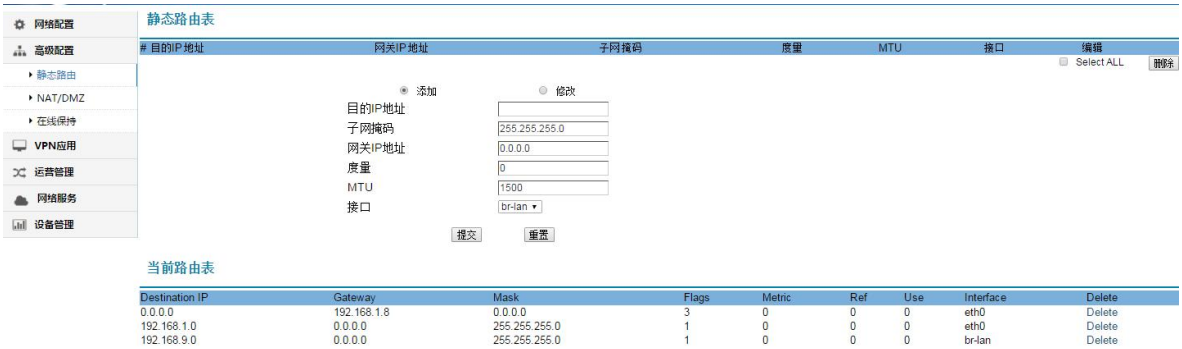


图 4-1-25

- **目的IP地址：** 路由的目的IP，可以是主机也可以是网段。
- **子网掩码：** 要添加的子网；如果是主机填写：255.255.255.255。
- **网关IP地址：** 要添加路由的下一跳IP，如果不需网关地址可使用“0.0.0.0”。
- **度量：**路由的度量值，默认为 0。
- **MTU：**路由的最大传输单元，默认值为1500。
- **接口：** 系统接口。

注：

无法成功添加路由，即添加规则成功后，路由信息没有出现相应的路由信息时，请确定网络号是否符合要求。

网关路由配置举例说明：

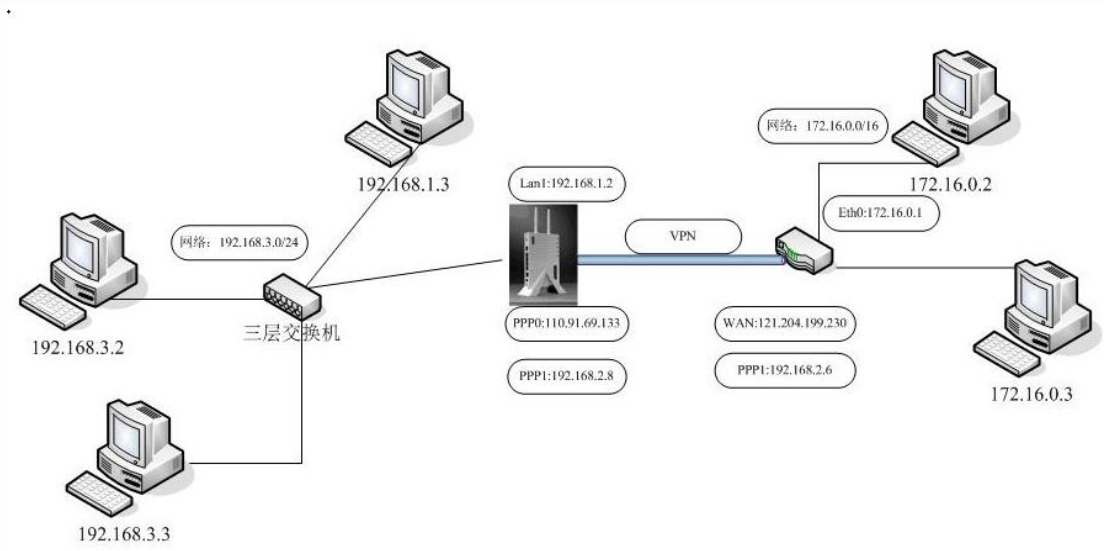


图 4-1-26

说明：图中有 192.168.1.0/24，192.168.3.0/24，192.168.2.0/24 三个网络。

192.168.1.2 为网关的以太网 LAN1-4 的 IP 地址；

110.91.69.133为无线网关无线拨号上网时运营商分配的PPP0的IP地址；

192.168.2.8 为网关的和服务器之间建立 VPN 隧道时出现的 PPP1 的隧道 IP 地址；

172.16.0.1 为 VPN 服务器的 ETH0 的 IP；

121.204.199.230为VPN服务器的公网IP；

192.168.2.6 为 VPN 服务器和无线网关之间建立 VPN 隧道时出现的 tunnel0 隧道的 IP 地址。

假设现在 IP 地址为 172.16.0.2 的主机想访问 IP 地址为 192.168.3.2 的主机，则需要在 VPN 服务器上添加一条访问 192.168.3.0/24 网络的路由。这条网关添加请参考服务器厂家提供的路由配置厂家说明书，或者询问服务器厂家提供商的技术支持人员。服务器的网关添加好后，同时需要在无线网关上添加两条路由：一条为外面数据包送往 192.168.3.0/24 主机的路由；另一条为 192.168.3.0/24 的内部网络主机送往 172.16.0.0/16 的路由。下列对网关的路由添加进行配置说明：

在无线网关上的“高级配置”里的“静态路由”加上下列规则：

图 4-1-27

其中 192.168.3.0 与网关的 LAN1-4 连接，所以接口需选择 br-lan。本条网关的功能是：把外面送往无线网关的目的 IP 地址为 192.168.3.0/24 的数据，送往 br-lan 接口，从而实现把数据包发送到 192.168.3.0 的内部网络。

图 4-1-28

本条路由的功能是：送往无线网关的数据包，如果目的 IP 地址为 172.16.0.0/24 网段，则把此数据包往 eth0 接口传送，同时这个数据包的网关 IP 地址为 192.168.2.6。这样通过这条路由，无线网关当收到目的 IP172.16.0.0/24 的数据包时，直接把数据包往 eth0 插口送，然后到达服务器 192.168.2.6，再通过服务器的路由把数据包路由到地址为 172.16.0.0/24 网段，从而完成数据包的全程路由工作。

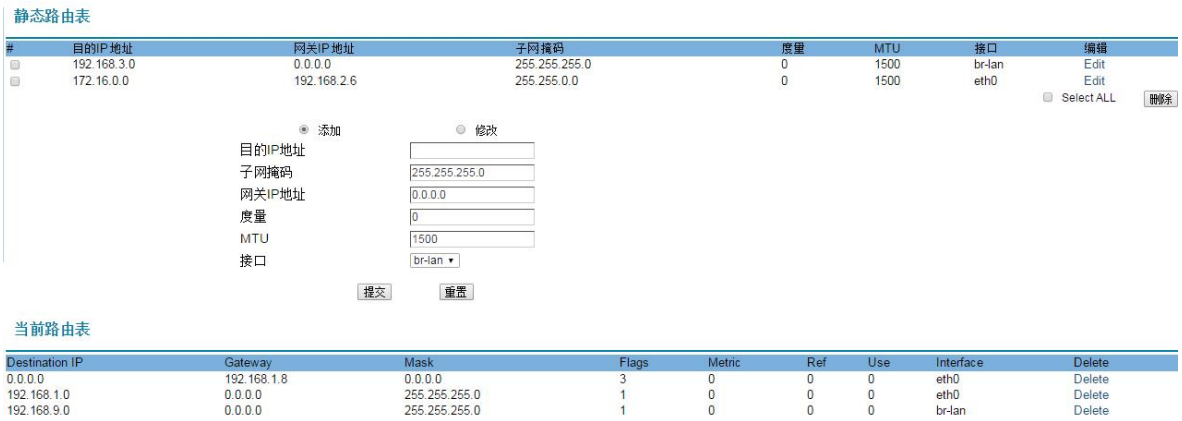


图 4-1-29

4.2.2 NAT/DMZ

4.2.2.1 NAT

NAT 英文全称是“Network Address Translation”，中文意思是“网络地址转换”或者说端口映射，顾名思义，它是一种把内部私有网络地址（IP 地址）通过不同的端口号映射成合法网络 IP 地址的技术。

图 4-2-1

通过设置规则，可以把外部网过来的数据，通过端口映射到指定的局域网某台 IP 地址的主机及端口上。

- **规则名**：限制可使用字符0-9.a-zA-Z，且不可以重名，作为区分多规则的标识。
- **协议**：数据包的协议：TCP/UDP、TCP、UDP。
- **外部区域**：即wan口。
- **外部端口**：外部过来的数据包TCP/UDP的端口值。
- **内部IP地址**：要映射的内部主机IP地址。
- **内部端口**：要做映射的内部主机服务的端口值。

4.2.2.2 DMZ

将一台局域网计算机完全暴露给 Internet，以实现双向通信，这时候就需要将该计算机设置成虚拟服务器（DMZ 主机）。当有外部用户访问该虚拟服务器所映射的公网地址时，设备会直接把数据包转发到该虚拟服务器上。

如果无线网关后面带的局域网内的某台 PC 机想和外网直接自由通行，可以简单快速启用 DMZ 的方式来实现。

图 4-2-2

设置方式是直接选择“启用DMZ”，然后目的地址中填入虚拟服务器的IP地址。点击“提交”即

可。

4.2.3 在线保持

图 4-2-3

在线维持功能是用来检测无线网关的在线状态，此功能会自动定期的监测无线网关和无线网络间的数据通道是否正常，发现异常，掉线了，软件会自动智能地重新拨号，实现设备无人看护下的永远在线，确保数据通道畅通。

客户请根据实际情况，填入稳定的“目的 IP 地址”和“目的地址端口”，作为在线维持的参考物。注意，填入的“目的 IP 地址”和“目的地址端口”务必是稳定的，因为无线网关是以这个服务器作为参照物的，如果这个服务器不稳定，会导致无线网关频繁掉线。检测间隔时间和检测超时次数选用默认值即可。

注意：

1、若未开启在线保持，则会导致无线网关掉线后无法重新启动的现象，就是掉线了不会重新上线。

2、填写的目的地址需稳定可靠，提供相应功能的服务。

3、在线保持默认是针对公网，在专网内需根据情况重新配置，如果不重新配置可能导致频繁掉线。

4.2.4 带宽管理

管理设备的带宽，支持对设备总带宽的设置和对某个 IP 段带宽的设置。

图 4-2-4

- **最大上行速度：**设置设备最大的上行速度。
- **最大下行速度：**设置设备最大的下行速度。
- **规则名：**标示添加规则的名称。
- **IP地址：**选择要限定的IP地址。
- **均分模式：**带宽是否均分。
- **上传带宽：**设置上传的最大带宽。
- **下载带宽：**设置下载的最大带宽。

4.3 VPN 应用

4.3.1 PPTP

PPTP是一个第2层的协议，将PPP数据帧封装在IP数据报内通过IP网络，如Internet传送。PPTP还可用于专用局域网络之间的连接。它使用一个TCP连接对隧道进行维护，使用通用路由封装（GRE）技术把数据封装成PPP数据帧通过隧道传送。可以对封装PPP帧中的负载数据进行加密或压缩。

图 4-3-1

- **服务器地址：** 服务器的ip或域名。
- **远程子网、远程子网掩码：** 服务器端的内网信息。
- **用户名/密码：** 接入到服务器的用户名和密码。
- **协议：** pptp进行ppp密码验证的方式。有以下认证方式：
  Pap：采用Pap认证方式，这种方式的用户名和密码是明文传送，安全级别低
  Chap：采用Chap认证方式
  MS-Chap：采用MS-Chap认证方式
  MS-Chap-V2：采用MS-Chap-V2认证方式
  Any：可能采用上面四种认证方式中的任何一种，没有特殊情况，请采用这个参数。
- **MPPE：** 加密方式，选择类型如下:
  NoMppe： 不提供MPPE加密。
  Mppe(40/128)： 提供MPPE功能，支持MPPE40、MPPE128加密方式。
  Mppe-StateFul： 提供MPPE stateful加密模式。
- **添加默认路由：** 如果启用，则所有访问本设备的数据，将全部发往PPTP隧道。在此情况下，本设备所带的主机，将只能访问VPN网络。
- **使能NAT：**如果启用，则本设备lan口局域网下的设备可以通过VPN隧道访问服务器。不启用，则局域网下的设备，无法通过VPN隧道访问服务器，只能通过外网访问服务器。
- **其他参数：**一般不需要填写，除非服务有要求特殊的协商参数。
- **指定本地IP/指定对端IP：**如果服务器端允许，本设备在建立ppp链路时，向服务器提出指定本地IP的请求，如果服务器给分配，则隧道建立将失败。
- **检测间隔时间（秒）/检测超时次数：**隧道一旦建立，本设备可以设定一定时间间隔（检测间隔时间），发送LCP包，检查链路。如果超过检测超时次数失败，则本设备将主动断开连接，重新请求建立连接。
- **其他协商参数：**用于链路建立时需要特殊参数进行协商的情况。一般不需要填写，除非服务有要求特殊的协商参数。参数格式如下：novj;novjcomp 参数间以”;”隔开。

注：

如果启用“默认路由”，所有的数据包将被转发到VPN服务器，即网关所带的设备将无法访问公网。请根据情况修改“在线保持”的参数。否则将导致频繁重拨。

4.3.2 IPSEC/L2TP

4.3.2.1 IPSEC

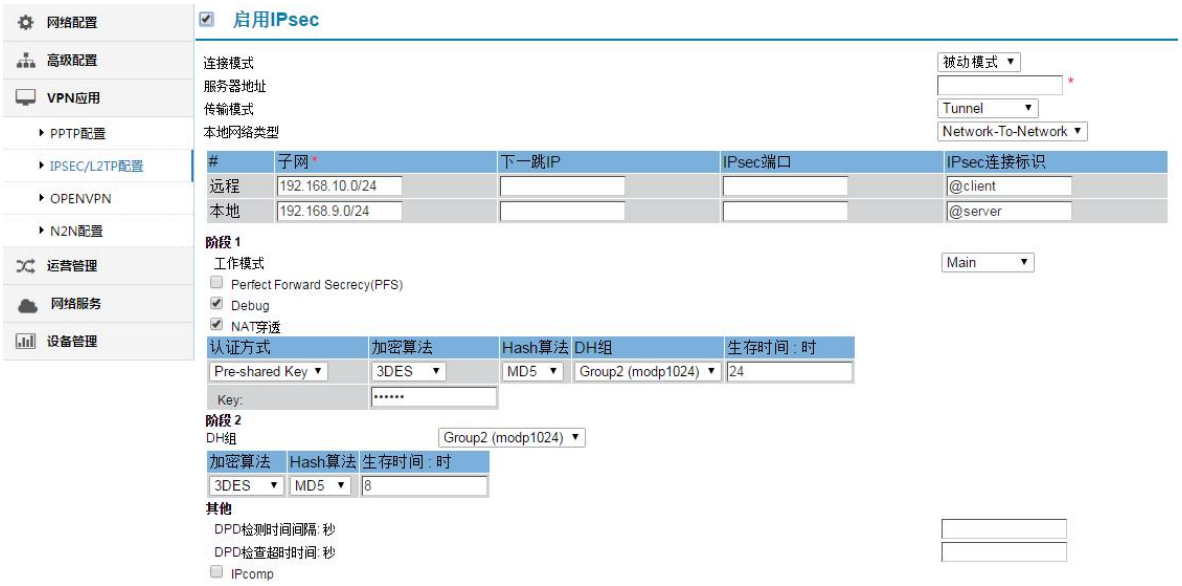


图 4-3-2

- **连接模式：**
  主动模式：由本端发起连接。
  被动模式：等待对方进行连接。
- **服务器地址：** 服务器的ip或域名（必填）。
- **传输模式：**
  Transport传输模式：一般应用为无线网关连接到服务器。
  Tunnel隧道模式：一般应用为两个网关间建立隧道。
  穿透模式Passthrough：允许IPSEC协议穿透。
- **本地网络类型：**
  Network-To-Network：用于网关所带子网内的设备与服务器所带的子网内的设备之间的通信。
  Road Warrior：作为移动客户端连接到服务器。
- **子网：** 当工作模式为Network-To-Network时，为双方所带子网。
- **下一跳IP：** 当设备处于内网，则此IP为设备所指向的网关的IP地址。
- **IPsec端口：** 当同时启用L2tp时，L2tp监听的端口。L2tp的端口默认是1701。
- **IPsec连接标识：** 用于连接协商时提供给对端的标识。

协商阶段1 ：第一阶段协商建立IPsec SA，为数据交换提供IPSec 服务。

- **工作模式：**Main 主模式、Aggressive模式。
- **PFS：** 精确转发保密。防止单密钥泄漏时，影响整个通信系统。
- **Debug：** 开启调试信息。
- **NAT穿透：** 如果本网关不是直接连接公网，而是经过IP源地址转发，则应该使用 “NAT穿越”。
- **认证方式：** Pre-shared Key预共享密钥模式、Certificates X509证书模式。
- **加密算法：** DES、3DES、AES和AES128。
- **Hash算法：** SHA1和MD5。
- **DH组：** Group1、Group2、Group5、Group14、Group15、Group16、Group17和Group18。

- **生存时间(秒)**：阶段协商有效时间。
- **Key**： 当认证模式为Pre-shared Key预共享密钥模式时，为共享密钥。
- **Password**： 当认证模式为X509证书时，证书的密钥。

协商阶段2：第二阶段协商消息受第一阶段SA 保护，任何没有第一阶段SA 保护的消息将被拒收。在第二阶段，快速快速协商通信协议算法，并交换密钥，建立通信。

- **DH组**： Group1、Group2、Group5、Group14、Group15、Group16、Group17和Group18
- **加密算法**： DES、3DES、AES和AES128。
- **Hash算法**：SHA1和MD5。
- **生存时间(秒)**：阶段协商有效时间。

其他参数

- **DPD检测时间间隔(秒)/DPD检测超时时间(秒)**：隧道一旦建立,本设备可以设定一定时间间隔(检测间隔时间)，发送LCP包，检查链路。如果超过检测超时时间失败，则本设备将主动断开连接，重新请求建立连接。
- **IPComp**： IP有效载荷压缩。

4.3.2.2 L2TP

L2TP（Layer Two Tunneling Protocol，第二层通道协议）是 VPDN（虚拟专用拨号网络）技术的一种，专门用来进行第二层数据的通道传送，即将第二层数据单元，如点到点协议（PPP）数据单元，封装在 IP 或 UDP 载荷内，以顺利通过包交换网络（如 Internet），抵达目的地。

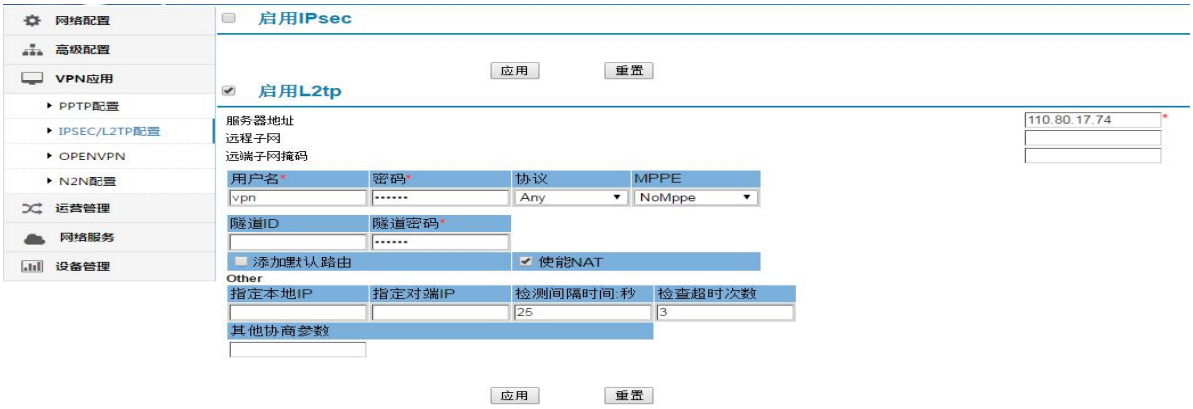


图 4-3-3

- **服务器地址**: 服务器的ip或域名。
- **远程子网、远程子网掩码**: 服务器端所带的子网信息。
- **用户名/密码**: LAC 帐号及密码。
- **协议**： pptp进行ppp密码验证的方式。有以下认证方式：
  Pap：采用Pap认证方式，这种方式的用户名和密码是明文传送，安全级别低
  Chap：采用Chap认证方式
  MS-Chap：采用MS-Chap认证方式
  MS-Chap-V2：采用MS-Chap-V2认证方式
  Any：可能采用上面四种认证方式中的任何一种，没有特殊情况，则默认采用。
- **MPPE**： 加密方式，选择类型如下:
  NoMppe： 不提供MPPE加密。
  Mppe(40/128)： 提供MPPE功能，支持MPPE40、MPPE128加密方式。
  Mppe-StateFul： 提供MPPE stateful加密模式。
- **隧道 ID/隧道密码**: LNS 帐号及密码。
- **添加默认路由**： 如果启用，则所有访问本设备的数据，将全部发往PPTP隧道。在此情况下，本

设备所带的主机，将只能访问VPN网络。

- **使能NAT：**如果启用，则本设备lan口局域网下的设备可以通过VPN隧道访问服务器。不启用，则局域网下的设备，无法通过VPN隧道访问服务器，只能通过外网访问服务器。
- **其他参数：**一般不需要填写，除非服务有要求特殊的协商参数。
- **指定本地IP/指定对端IP：**如果服务器端允许，本设备在建立ppp链路时，向服务器提出指定本地IP的请求，如果服务器给分配，则隧道建立将失败。
- **检测间隔时间（秒）/检查超时次数：**隧道一旦建立，本设备可以设定一定时间间隔（检测间隔时间），发送LCP包，检查链路。如果超过检测超时次数失败，则本设备将主动断开连接，重新请求建立连接。
- **其他协商参数：**用于链路建立时需要特殊参数进行协商的情况。一般不需要填写，除非服务有要求特殊的协商参数。参数格式如下：novj;novjcomp 参数间以”;”隔开。

4.3.3 OPENVPN

OpenVPN 是一个基于 OpenSSL 库的应用层 VPN 实现。和传统 VPN 相比，它的优点是简单易用。

图 4-3-4

- **服务器地址**：服务器的ip或域名。
- **协议**：TCP或UDP协。
- **设备**：tun或tap。

协议和设备必须与服务端配置相同。

客户端设置：将服务端生成的的 ca.crt 、client.crt 、client.key 这三个文件打包好发给客户端，客户端路由设备分别上传三个文件。

图 4-3-5

上传成功

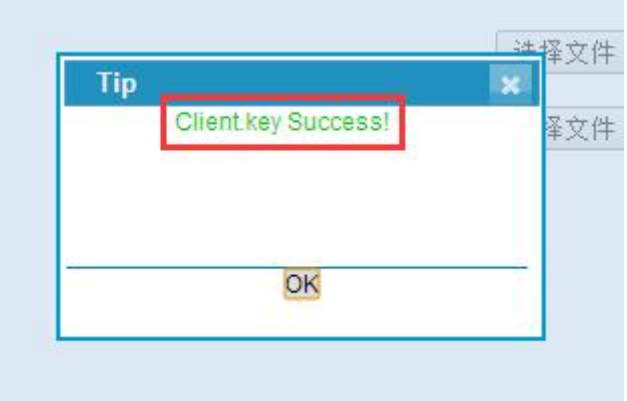


图 4-3-6

填写客户端配置信息。

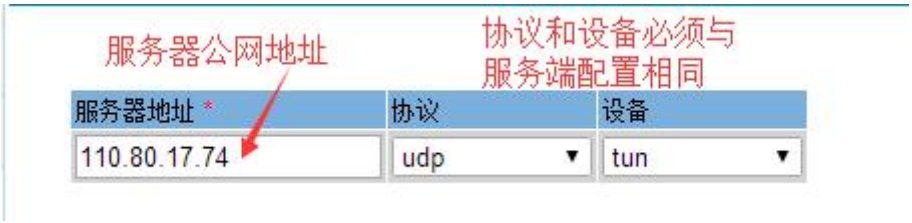


图 4-3-7

在服务端开启后，点击 OPENVPN 的“启用”按钮即可连接。

4.3.4 N2N

N2N 是一个双层架构的 VPN，它让用户可以在网络层上开发 P2P 应用的典型功能，而不是在应用层上开发。这意味着用户可以获取本地 IP 一样的可见度（比如说，同一个 N2N 网络内的两台 PC 机可以相互 ping 通），并且可以通过 N2N 虚拟网内的 IP 地址相互访问，而不必关心当前所属的物理网络地址。可以这样说，OPENVPN 是把 SSL 从应用层转移到网络层实现（比如说实现 https 协议），而 N2N 则是把 P2P 的实现从应用层转移到网络层。

图 4-3-8

- **接口名称**：自定义接口名称。
- **本地IP地址**：隧道口IP地址。
- **子网掩码**：子网掩码。
- **社区名称**：连接的组名称。
- **社区密码**：连接的组密码。
- **服务器IP地址**：服务器地址。
- **服务器端口**：服务器端口。
- **物理地址**：接口对应的物理地址。
- **MTU**：最大传输单元。

4.4 运营管理

4.4.1 WiFidog 认证配置

WiFidog 功能，用于实现网页认证功能，当用户连接到无线热点，发出数据请求时，会首先打开所配置的鉴权服务器地址所在路径下的认证页面让用户进行认证，当认证通过后，方可正常上网。

图 4-4-1

- **工作模式选择：**主要有普通认证、微信认证、工业路由和本地认证。
- **网关ID：**WiFidog上传消息给服务器时附带的网关标识。
- **WEB服务器名：**用户自定义的服务器的名称。
- **外出接口：**设备的总数据接口。
- **内部接口：**用户数据的接口。
- **WiFidog端口：**WiFidog使用的端口号。
- **最大并发用户数：**最大的用户同时请求数量。
- **检测间隔时间（s）：**检测用户流量信息和设备状态的时间间隔。
- **用户超时检测次数：**判定用户超时的检测次数。
- **用户上网时长（s）：**用户认证通过之后免认证上网时长。
- **鉴权服务器地址：**认证服务器的地址。
- **启用SSL：**对接服务器是否使用SSL解密。
- **鉴权服务器端口：**服务器使用的端口号。
- **鉴权服务器路径：**服务器端的鉴权路径，路径两侧要加‘/’。
- **定点推送广告：**选择是否定点推送广告。
- **是否上传浏览记录：**选择是否上传用户浏览的URL记录。
- **域白名单：**WiFidog不屏蔽的域名地址，规则格式为 FirewallRule allow tcp to XXX 。

4.4.2 应用层过滤

设置对用户的某些应用进行过滤，可以对视频，音乐，下载，URL 等进行过滤。

图 4-4-2

- **规则名：**标示限制规则的名称。
- **IP范围：**对IP段进行限制。
- **协议类型：**选择要过滤的协议的类型（视频，音乐，下载等）。
- **数据包的方向：**选择要过滤的数据来源，IN,OUT,IN/OUT。
- **策略：**对规则匹配到的数据处理的策略，接受或禁止。

4.4.3 如影随形

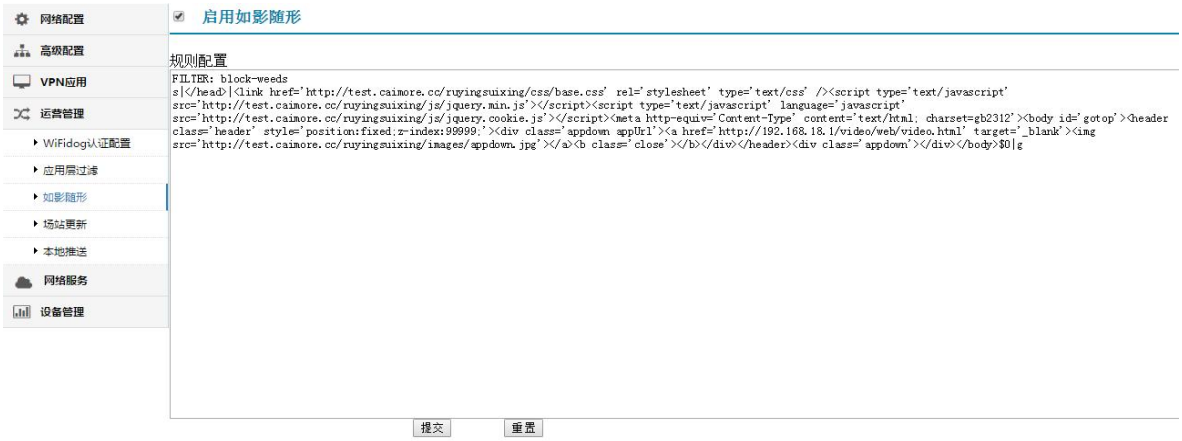


图 4-4-3

- **启用：**启用如影随行的功能。
- **规则配置：**配置页面替换的内容，也就是页面插入广告内容，规则的第一行：FILTER: block-weeds；第二行：正则表达式规则，如s|页面内容|替换内容$0|g。
  启用后在设备连上该无线的时候，浏览网页的过程中可在网上最上方看到该广告。

4.4.4 场站更新

图 4-4-4

- **场站ESSID：**需要连接的场站WiFi的网络标识。
- **场站ESSID密码：**场站WiFi的密码。
- **多媒体服务器IP：**选择要连接的服务器IP，这边需要与WiFi同一局域网。
- **多媒体更新段：**服务器上面配置的更新段名。
- **设备更新目录：**更新到设备的本地路径。
- **更新用户名：**服务器分配的用户名。
- **更新密码：**服务器分配的用户名所对应的密码。
- **扫描频率（秒）：**扫描WiFi的时间间隔。

4.4.5 本地推送

图 4-4-5

- **启用：**开启本地推送。
- **广告名：**自定义广告名。
- **广告URL：**需要推送的URL地址。
- **推送频率：**推送广告的时间间隔。

4.5.1 动态 DNS

DDNS 是将无线网关拨号获得的动态 IP 地址映射到一个固定的域名上，实现无线拨号获得的可能不断变化的 IP 地址和固定不变的域名之间的绑定。

如果无线网关有启用动态域名解析，则无线网关每次拨号成功获得新的 IP 地址后，会把新获得的动态 IP 地址发送到客户配置的动态域名解析服务器上去，实现动态域名解析服务器上设置的域名和本网关 IP 地址之间绑定的更新。

启用动态域名解析功能，可以解决因为无线网关每次拨号获得 IP 地址不同，而无法作为服务器使用的缺点；如果客户需要把无线网关作为服务器来使用，和客户端的设备通信（比如 DTU），则需要启动本动态域名解析功能,同时客户端设备则需要把动态域名填入到对应的配置选项,这样客户端设备,每次要和无线网关通信前,会从域名服务器先会通过域名解析获取无线网关的 IP 地址，然后根据获得变动后的无线网关的 IP 地址来通信。

图 4-5-1

- **接口：**可选择wan、lan、4g、vpn四种接口。
- **服务：**选择服务后需先登录对应的网址进行用户注册和域名注册，然后根据注册获得的域名、用户名和密码信息填入到对应输入框,然后点击“提交”,保存参数。(如服务选择“dyndns.org”,则需先登陆到“www.dyndns.com”进行用户注册和域名注册）。
- **主机名：**DDNS的域名。
- **用户名：**登录dyndns服务器的用户名。
- **密码：**登录dyndns服务器的密码。
- **IP地址来源：**可选择网络、接口、URL。
- **URL：**所使用的服务器地址。
- **检测IP变动的时间间隔：**检测IP变动的时间间隔值。
- **时间单位：**可设为分、时。
- **强制更新间隔：**强制更新的时间间隔。
- **强制更新的时间单位：**可设为分、时。

4.5.2 花生壳内网版

花生壳分为两类：公网版花生壳和内网版花生壳。公网版花生壳功能即动态域名解析功能，需要提供一个公网ip地址，可以用域名来绑定这个公网地址，从而实现远程访问路由器。内网版花生壳需要提供一个开通了内网穿透的花生壳账户。在没有公网ip地址的条件下，通过该账户去关联设备来实现远程访问路由器或者路由器下的终端设备。

图 4-5-2

点击启用并提交，刷新页面后状态显示为online，并自动获取一个SN码，这个SN码由设备MAC地址通过计算方式计算出来的，只要设备的MAC地址唯一，则设备的SN码唯一。点击登录管理后会跳出SN码登录页面：

图 4-5-3

SN码会自动从登录页面获取，初始密码为admin,点击登录后会弹出：

图 4-5-4

可在该窗口设置登录密码作为之后登录使用，提交后会显示激活成功，如下图：

图 4-5-5

登录后会显示一个域名，为该设备动态DNS域名，如果该设备是直接使用公网ip上网，那么访问该域名就相当于访问这台路由器，如果路由是使用局域网上网（大多数SIM卡也属于局域网），那么要实现通过访问域名来访问路由器或者路由器LAN口下的设备，那么该账号要关联一个已开通内网穿透的花生壳账户，则可实现内网穿透功能。操作如下：

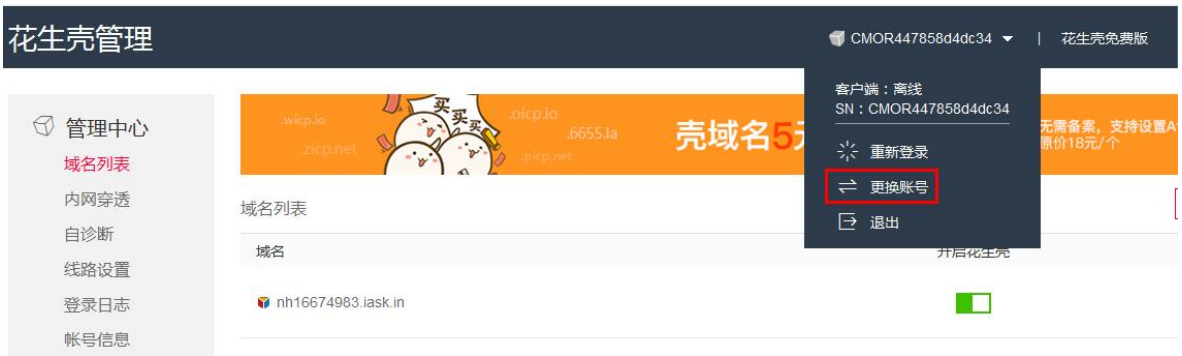


图 4-5-6

图 4-5-7

4.5.3 流量监控

要开启流量监控之前，一定要先在 WiFi 探针中同步一下时间，保证设备的时间是当前的正确时间。

图 4-5-8

- **统计清零：**可将统计的设备使用流量全部清零。
- **流量阀值（MB）：**设定时间内流量的最高使用量。
- **流量统计周期：**可选择每日或每月进行流量统计。
- **流量超出后相应：**可选择关闭WiFi、关闭有线网络、关闭WiFi和有线网络、关闭3G/4G。
- **上报流量：选择是否将**设备统计的使用流量上报给服务器。
- **白名单：**（注意！仅在关闭3G/4G时使用）在白名单中输入网址，在超出限制是任然可以访问。单击提交，统计的流量会重置。

4.6 设备管理

4.6.1 状态查询

显示系统状态、外网口状态、内网口状态、WiFi 状态、VPN 状态等信息。如图：

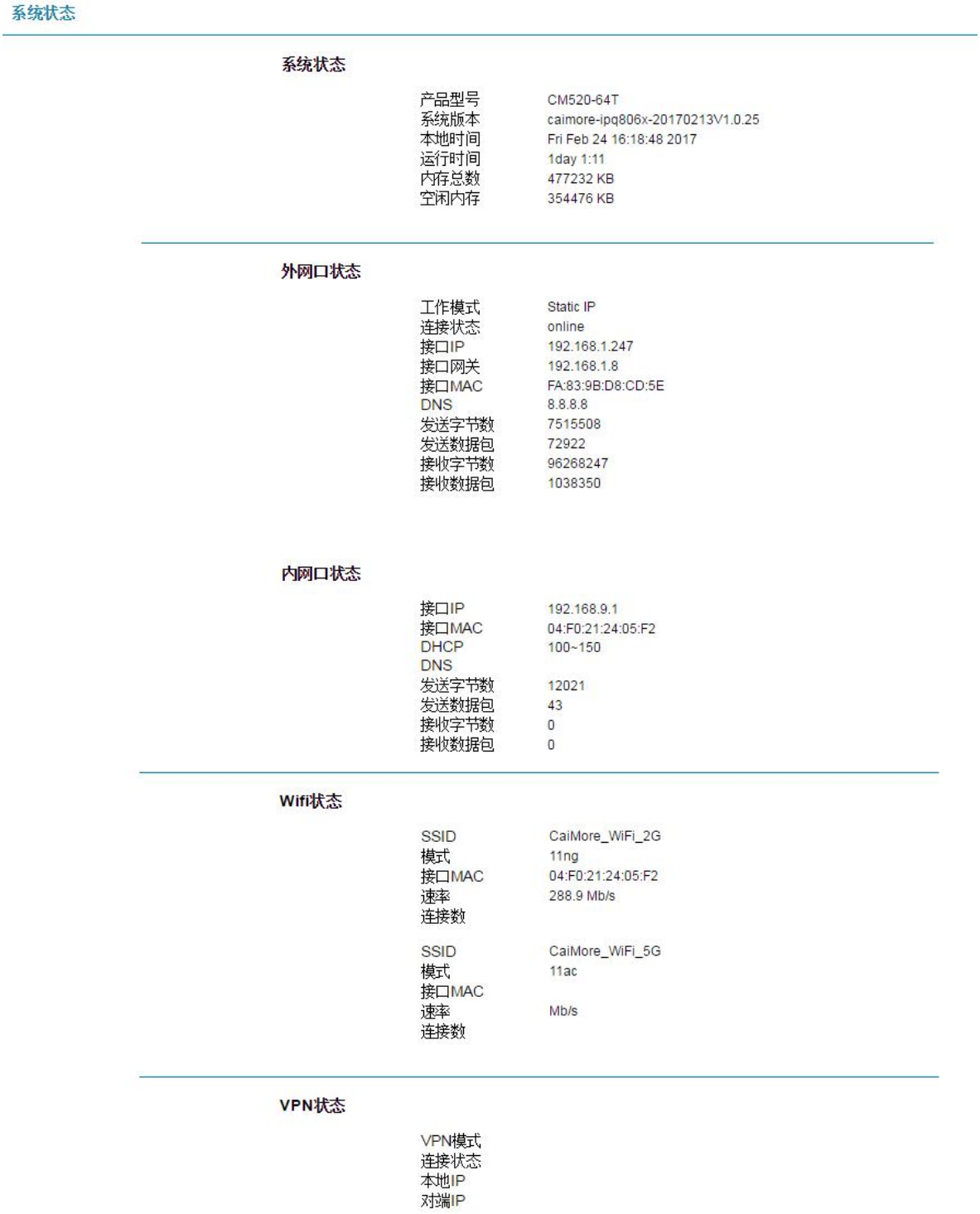


图 4-6-1

4.6.2 日志信息

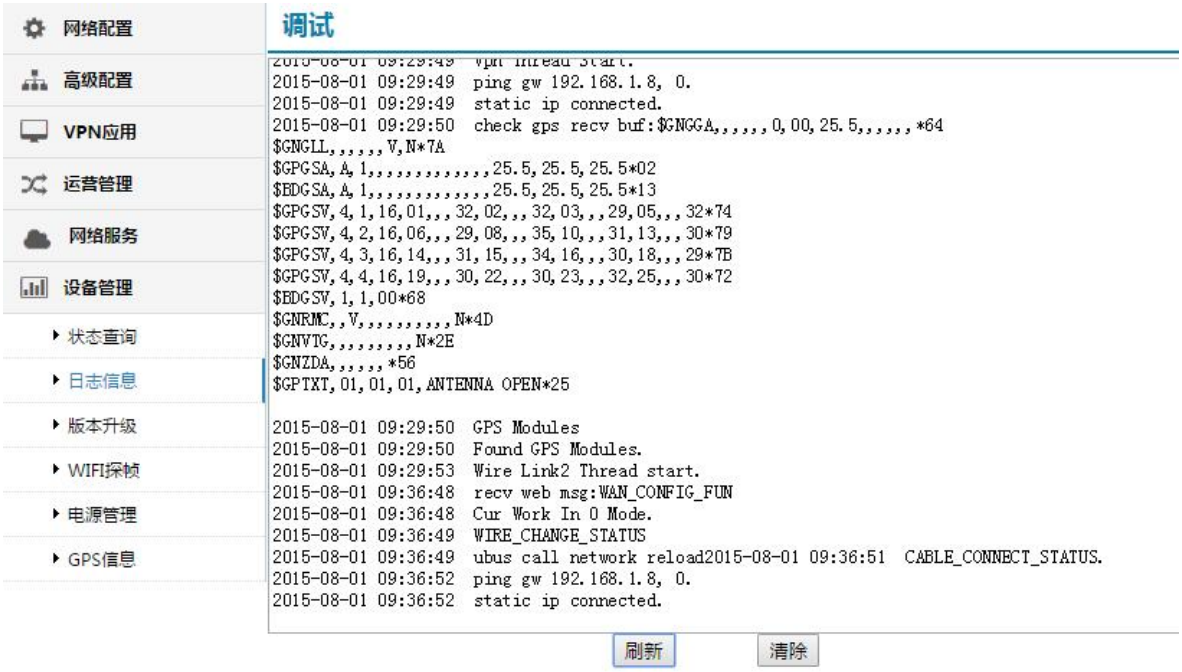


图 4-6-2

- **刷新：**点击该按钮可调取设备的调试信息。
- **清除：**点击该按钮可将窗口的调试信息全部清除。

4.6.3 版本升级

图 4-6-3

- **是否保存配置参数：**可选择是否保存以保存的参数配置。
- **路由器升级版本：**点击“选择文件”按钮，可选择需升级的文件（文件由厂商提供）。点击“提交”按钮，设备将开始升级，升级过程中设备会自动重启，请勿断开电源。
- **恢复出厂设置：**点击“恢复”按钮，设备将会自动重启并恢复出厂设置。

4.6.4 WIFI 探帧

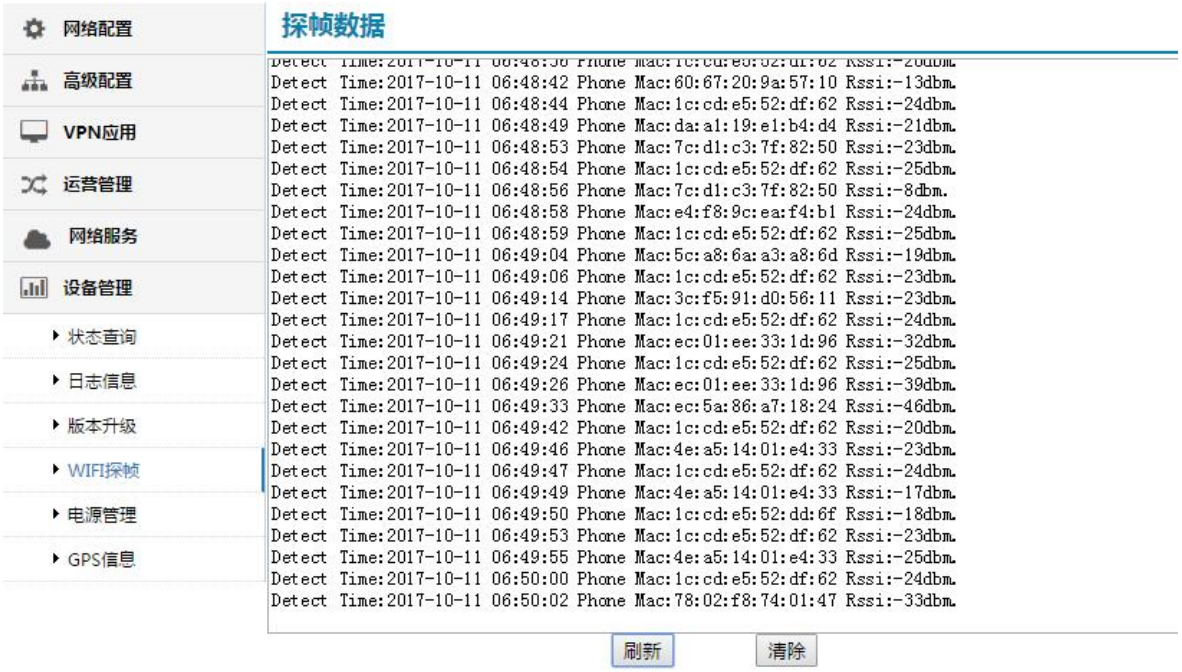


图 4-6-4

- **探帧数据：**可显示抓取的帧数据以及信号强度。

4.6.5 电源管理

图 4-6-5

- **当前时间：**可显示设备的当前时间。
- **校准模式：**时间校准模式，分网络和手动。
- **手动设置：**可以手动设置设备时间。
- **模式：**默认为每日。
- **开机时间：**设备正常工作时间。
- **关机时间：**设备进入低功耗模式时间。

4.6.6 GPS 信息

图 4-6-6

当设备带有 GPS 功能时用于显示设备获取的经纬度信息。

- **经度：**当前设备所在的经度。
- **纬度：**当前设备所在的纬度。

第五章 常见问题

1. 频繁上下线

- 请进入系统状态查看网络信号，是否网络信号值太低。
- 请检查在线保持的相关参数，规则是否满足导致下线。
- 如果在线保持目的 IP 使用域名，请登录网关的命令终端（附录 1）确定是否能正常解析域名和访问目的地址。

2. 忘记密码

- 请恢复出厂，请参看（附录 4）。

3. LAN 灯不亮

- 请查看网线是否与设备紧密相连。
- 如果是网关与 PC 直接相连接请更换交叉数据线。
- 把网关与交换机相连接，查看网线路是否正常。

4. 无法拨号上网

- 请查看 WAN 配置的信息是否与运营商提供的一致。
- 通过系统状态查看信号，如果信号值低，请检查天线是否正常连接。
- 查看该位置是否有网络覆盖。
- 通过系统状态查看信号和卡的状态，如果卡状态错误，请重新插卡或更换卡。

5. 已经拨号上网，但无法打开网页

- 请检查设备的网关是否指向路由器。
- DNS 是否与路由器的一样。如果不一样请修改（参见附录 5）。
- 如果有填写 DNS 请检查填写的信息是否正确。
- 如果填写 DNS 是正确，请先清空（使用自动获取 DNS），拨号成功后，再根据系统状态提示的 DNS 写入设备。

附录 1　使用 ssh 登录网关命令行终端

1、双击 

，打开 Xshell：

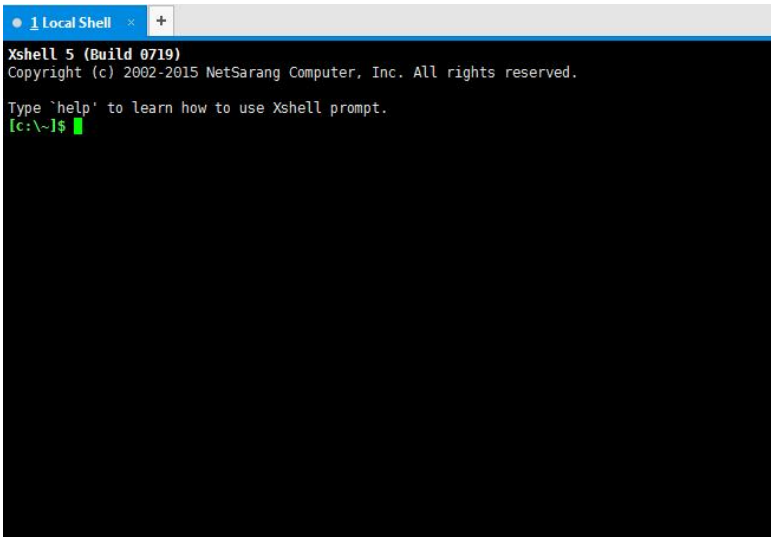


图 a1-1

2、在弹出的界面里输入：ssh 192.168.9.1（网关的 IP）<回车>：

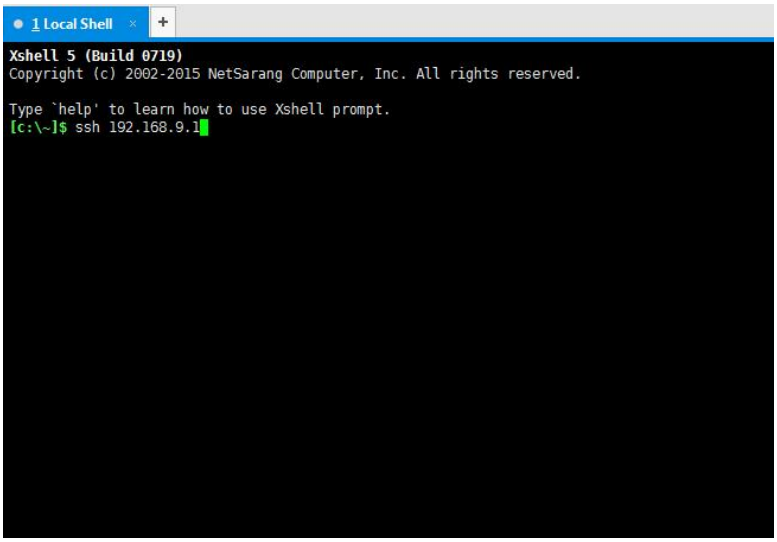


图 a1-2

3、输入依次弹出的窗口中分别输入用户名和密码：

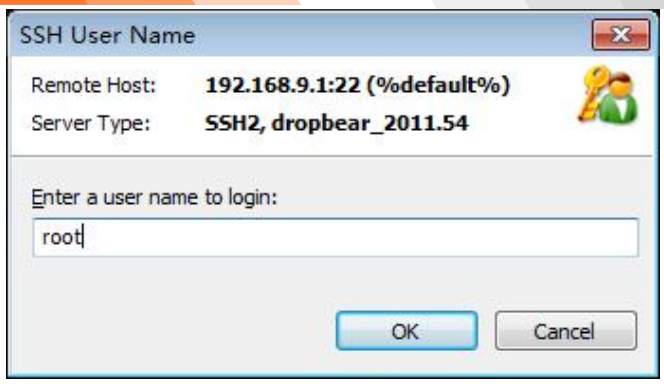


图 a1-3

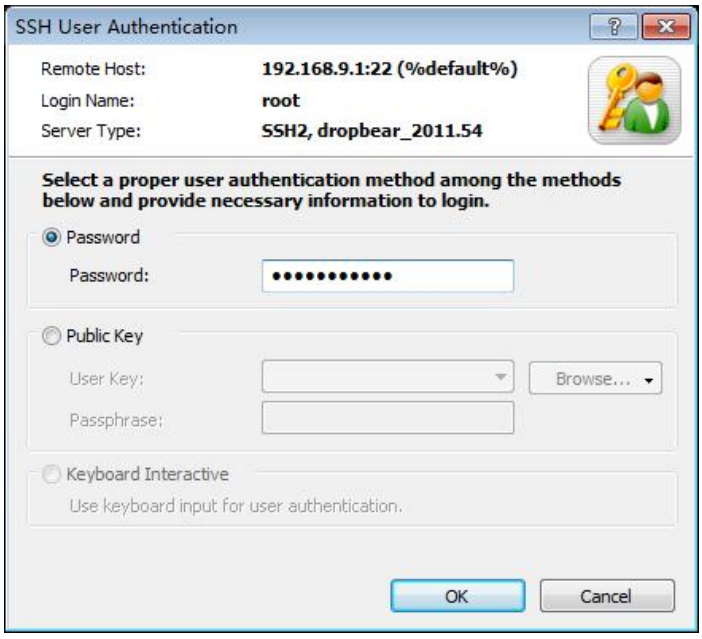


图 a1-4

4、出现下图表示登录成功，进入 shell 命令。

图 a1-4

附录 2　使用串口登录网关命令行终端

1、双击 

，打开 Xshell：

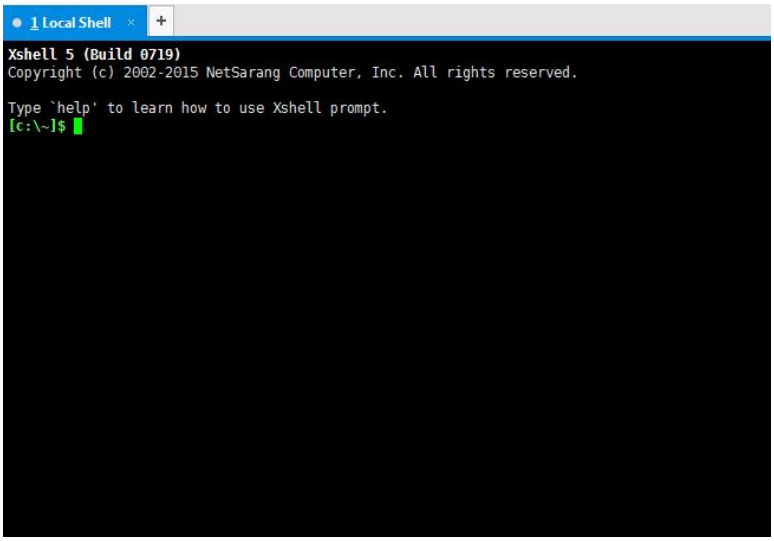


图 a2-1

2、新建一个会话控制，设置相应参数：

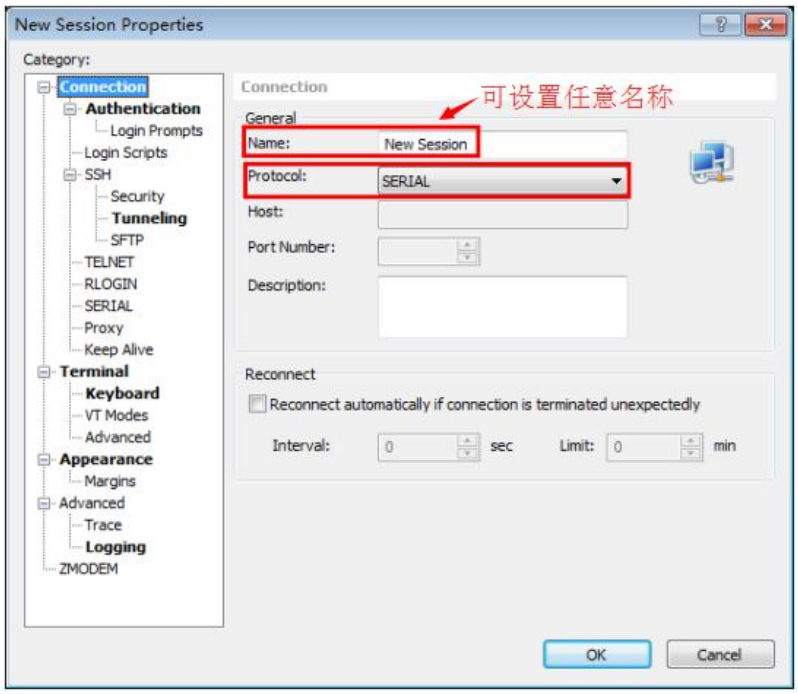


图 a2-2

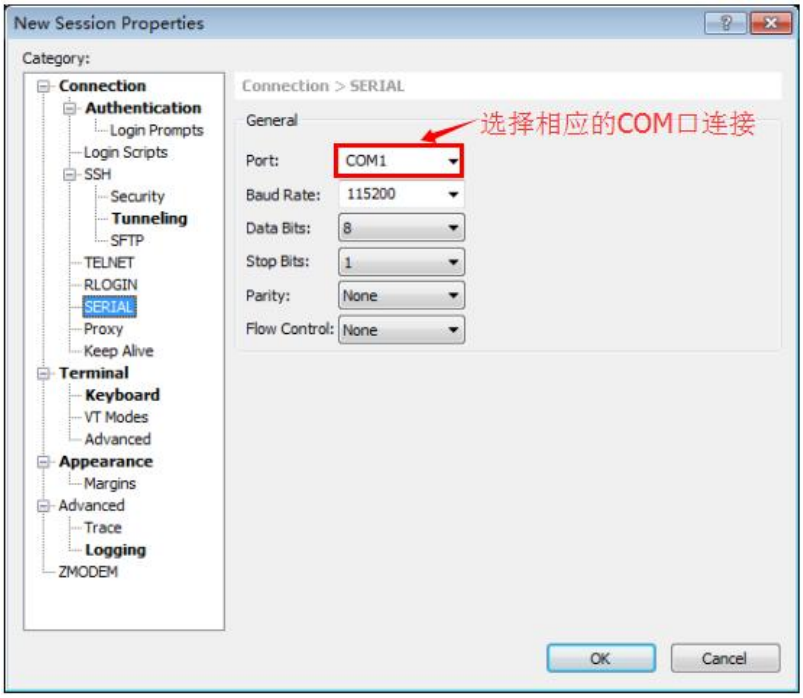


图 a2-3

3、确定进入该页面：

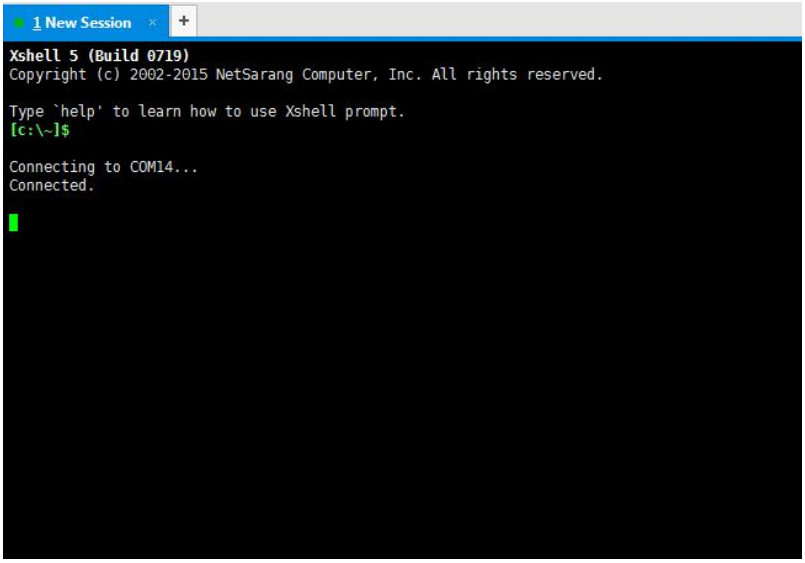


图 a2-4

4、< 回车 >，提示登录对话框，输入用户名和密码：

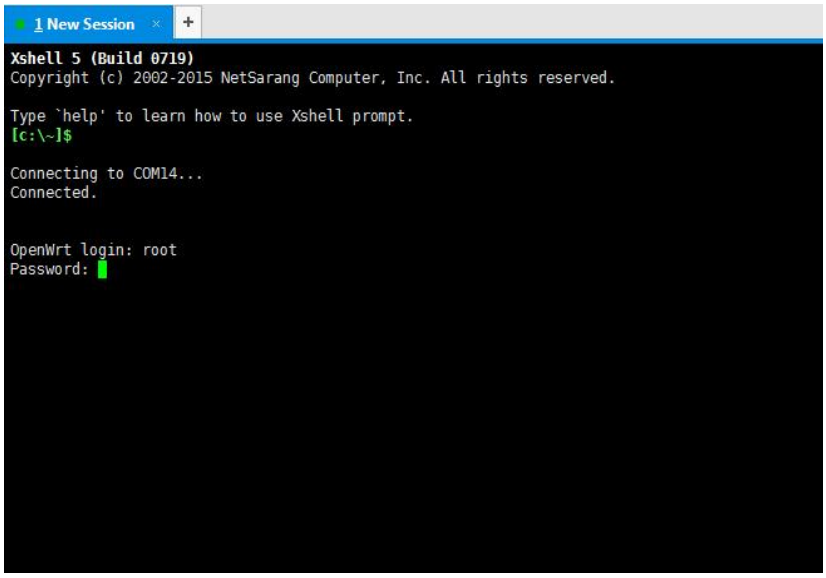


图 a2-5

5、出现下图表示登录成功，进入 shell 命令。

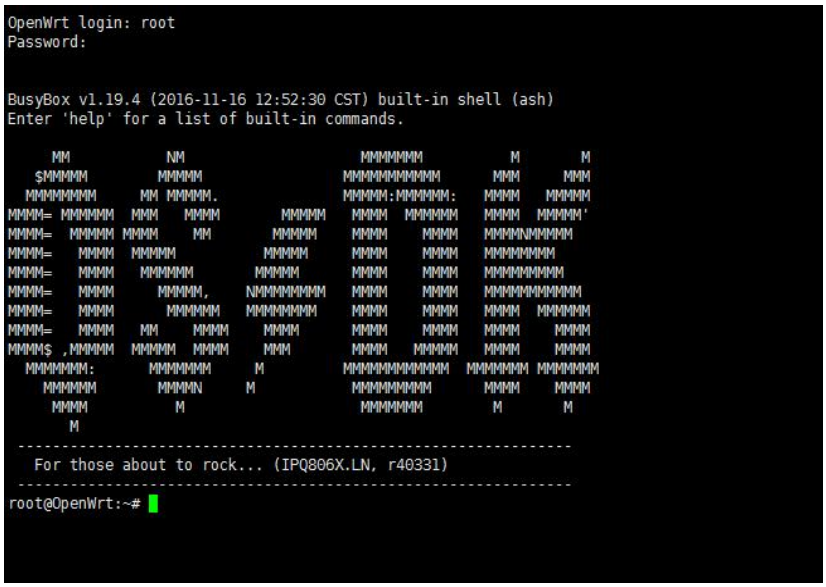


图 a2-6

附录 3　恢复出厂设置

1、给设备上电。
2、按住 RESET，约 3 秒。
3、设备所有的指示灯全亮，然后松开按键
4、设备进入复位状态并自动重启

附录 4　无线网络基本信息

网络	中心号码（APN）	接入点	用户名	密码
GPRS	*99***1#	cmnet(移动) uninet(联通)	为空	为空
EDGE	*99***1#	cmnet	为空	为空
TD-SCDMA	*98*1#	cmnet	为空	为空
CDMA	#777	为空	card	card
EV-DO	#777	为空	card	card
WCDMA	*99#	3gnet	为空	为空

注意：3G以上面为例，4G默认放空。本节提供的中心号码,接入点信息仅供参考，如有冲突与运营商提供的为准。正常情况下使用我们公司出厂的默认参数就可以,不用修改，只有使用APN/VPDN专网才需要修改这项配置。

附录 5　根据网关获取的 DNS 设置

进入网关的系统状态，查看 DNS：

图 a5-1

点击“开始” → “控制面板”，点击“网络连接”，如图：

图 a5-2

右键点击“本地连接”，选择“属性”，选择“Internet 协议 (TCP/IP)”，点击“属性”，将弹出如下配置窗口，根据网关的系统状态提示的 DNS 进行修改，修改完成后，点击“确定”

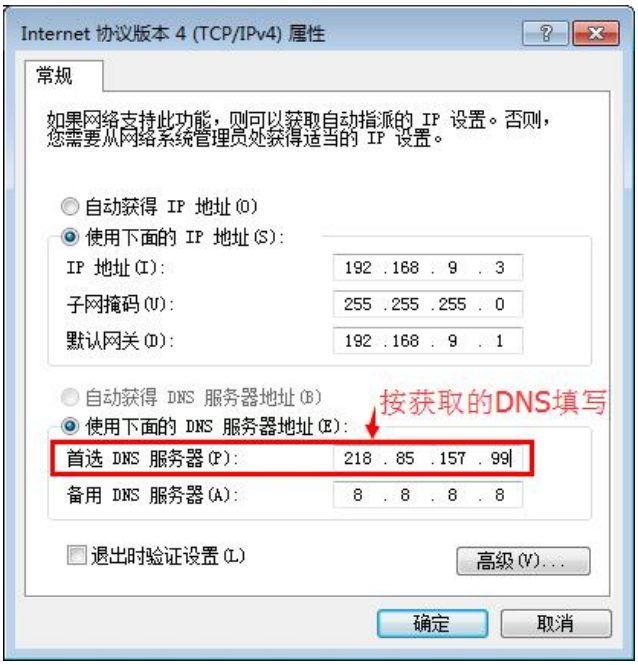


图 a5-3

厦门才茂通信科技有限公司

电话：0592-5902655　传真：0592-5975885 邮政编码：361009

网址：www.caimore.com Email:caimore@caimore.com

----有限生命 无线精彩----